Child Online Safety: A Select Study in Indian Context

Thesis

submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

by

DITTIN ANDREWS

SCHOOL OF MANAGEMENT

NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA,

SURATHKAL, MANGALORE – 575025

DECEMBER, 2021

Child Online Safety: A Select Study in Indian Context

Thesis

submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

by

DITTIN ANDREWS

(155057HM15P01)

Under the guidance of

Dr. Sreejith A

SCHOOL OF MANAGEMENT

NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA,

SURATHKAL, MANGALORE – 575025

DECEMBER, 2021

DECLARATION

I hereby *declare* that the Research Thesis entitled "**CHILD ONLINE SAFETY: A SELECT STUDY IN INDIAN CONTEXT,"** which is being submitted to the **National Institute of Technology Karnataka, Surathkal,** in partial fulfilment of the requirements for the award of the Degree of **Doctor of Philosophy in Management** is a *bonafide report of the research work carried out by me*. The material contained in this thesis has not been submitted to any University or Institution for the award of any degree.

Mr. Dittin Andrews
Reg. No.: 155057HM15P01
School of Management

Place: NITK, Surathkal
Date: 08-12-2021

CERTIFICATE

This is to *certify* that the Research Thesis entitled **"CHILD ONLINE SAFETY: A SELECT STUDY IN INDIAN CONTEXT"** submitted by Mr. Dittin Andrews (Register Number: 155057HM15P01) as the record of the research work carried out by him, is *accepted as the Research Thesis submission* in partial fulfilment of the requirements for the award of degree of Doctor of Philosophy.

Dr. Sreejith A
Research Guide
Assistant Professor
School of Management
NITK, Surathkal - 575025

Rajesh H.
Head, School of Management
National Institute of Technology Karnataka
Post Srinivasnagar,Surathkal D.K.-575025

Chairman, DRPC
(Signature with Date and Seal)

DEDICATION

This thesis is dedicated to my beloved parents, wife, and lovely children

ACKNOWLEDGEMENT

I express my sincere gratitude to my research advisor **Dr. Sreejith A**, Assistant Professor, School of Management, National Institute of Technology Karnataka (NITK), Surathkal, for his constructive support and guidance throughout my study, research, and thesis writing. His ideas, support, and words of wisdom have helped me immensely sail through my Ph.D. journey. I thank him for introducing me to various concepts, views, and people, as they have helped me broaden my perspective towards academics, research, and life in general. Under his supervision, my takeaway is not only a Ph.D. degree but also a different outlook towards research and leadership. I am also very thankful to him for giving me space and freedom to explore my areas of interest and work on them. Thanks to Dr.Sreejith that I can call my Ph.D. journey an enjoyable one. I will remain highly indebted to him for being very patient and understanding in mentoring me.

I whole-heartedly thank my Research Progress Assessment Committee members, **Dr. Jidesh P**, Assistant Professor, Department of Mathematical and Computational Sciences, NITK, Surathkal, and Prof. **K B Kiran** Professor and former Head of the department, School of Management, NITK, Surathkal, for their guidance at each step of my study which has helped me in making this research better. I would also like to thank our former secretaries **Dr. Savita Bhat** Assistant Professor, School of Management, NITK, Surathkal, and **Dr. Suprabha K. R**, Assistant Professor, School of Management, NITK, Surathkal.

I am highly grateful to **Dr. Rajesh Acharya H**, Head & Associate Professor, School of Management, NITK Surathkal, and our previous heads of the department, **Prof.Aloysius Henry Sequeira**, Professor, School of Management NITK, Surathkal and **Dr. S Pavan Kumar Associate Professor,** School of Management NITK, Surathkal for their support in the successful completion of this research work. I also express my gratitude to all the **Faculty Members** in the School of Management, NITK Surathkal, for their kind help.

I take this opportunity to thank **Dr.N Sarat Chandra Babu**, former Executive Director at Centre For Development of Advanced Computing, Bangalore, for granting permission for my research study. Also, I would like to thank **Shri. Gangaprasad GL** and **Shri. B S Bindumadhava,** former Centre Heads C-DAC, Bangalore. I am incredibly thankful to **Dr. Kumari Roshni VS** former Group Head, Cyber Security Group CDAC Bangalore, for her support during the initial stages of my research. I also thank **Dr.Subramanian N**, Senior Director Corporate R&D, for his sincere feedbacks and motivation. I am very much thankful to **Ms.Ananthalakshmi Ammal**, former Group Head Cyber Security group CDAC

Thiruvananthapuram for her valuable support and feedback during the final stage of my research. I want to extend my sincere gratitude to **Shri. Magesh Ethirajan**, Executive Director CDAC Thiruvananthapuram and **Shri. Satheesh G**, Group head Cyber Security, CDAC Thiruvananthapuram.

I want to thank my colleagues at CDAC Electronic City Bangalore and Technopark Thiruvananthapuram **Mr.Muraledharan N, Mr.Praveen D Ampatt, Dr.Sreekanth NS, Ms.Nobby Varghese, Ms.Indu Sasidharan, Ms.Anna Thomas, Mr.Senthilkumar KB, Mr.Sibi C Joseph, Mr.Bejoy Dickson, Mr.Jyothish J, Mr.Nabeel Koya, Mr.Aneesh Kumar KB, and all my team members** for all the chats and positivity during a stressful time.

I wish to thank my fellow research scholars **Mr.Naganna Chetty, Dr.Rajesh R Pai**, **Ms**. **Vanitha P. S, Mr. Jayan V**, and others, for their help. I extend my immense gratitude to my **Teachers, Colleagues, and Friends** at NITK Surathkal and CDAC Centres at Electronics City, Knowledge Park, and Thiruvananthapuram for their professional guidance, support, and unlimited motivation. I must thank the **Students, Parents, IT Professionals, and Legal Professionals,** whose cooperation and inputs made the research a successful one. My special thanks to all **administrative divisions** and **Supporting Staff** at NITK Surathkal and CDAC for helping me during these years of my study, both academically and officially. I extend my sincere thanks to all persons who contributed to this thesis and whose names could not be documented one way or the other.

My special thanks to my wife, **Dr. Smitha,** my children **Ann Elsa, Mikhail,** and **Athena Merryl,** who bear with me patiently and for their strong support. I express my heartfelt thanks to my **parents, Sisters, and in-Laws** for their prayers and motivation.

Last but not least, I thank **God Almighty** for the blessings He bestowed upon me and for giving me the strength and wisdom to reach this milestone in my life.

Dittin Andrews

EXECUTIVE SUMMARY

The exponential rise in mobile and Internet technologies and allied applications has broadened the horizon for different stakeholders to employ it for fulfilling personalized demands. In recent years the use of the Internet in youngsters below Eighteen has increased exponentially. Internet does have a positive role for children with the possibility of getting in contact with malicious users or ill-web content. Children are not covered with a shield against age-inappropriate content. The preparation of standards and guidelines for children or young people, parents, caretakers, pedagogues, policymakers, and industry is taken up by few international research organizations.

The principal goal of this research is to assess the perception of the different stakeholders to understand root causes, behavioral perception, and possible solutions to avoid online cybercrime and (online) child exploitation. The research analyses the identified research objectives. (1) To examine the specific issues pertinent to online child safety and protection; (2) To analyze the adult content identification mechanisms based on E-discovery techniques; (3) To explore the existing global practices addressing Child online safety; (4) Study and examine a risk mitigation framework addressing children online issues in the Indian Context.

This study can be stated as a behavioral assessment paradigm where the respective perception of the allied stakeholders has been assessed to identify key factors that impact the techniques and decisions to prevent online child exploitation. The overall research intends to assess different causative factors of online child exploitation, risk mitigation, and preventive approaches to avoid online child exploitation. To meet the objectives of the study, both primary and secondary data have been collected. Semi-structured questionnaires have been constructed and administered. The research identified different factors that influence child online safety and confirms some factors as predictors of child online safety.

The current study addresses the synthesis of three case studies in detail: (i) Lab setup providing test results of various commercial and open-source electronic discovery applications;(ii) Analysis of online social media responses and awareness posts on children online safety; (iii) Study on cyberbullying detection in social media text messages.

Considering the inevitable significance of online child exploitation events in present-day scenarios, a mixed research paradigm was applied to understand the causes and avoidance of online child exploitation and risk mitigation measures. This study found that apart from content filtering and parental control, access-log exchange, data access sharing, and inter-channel coordination amongst the different stakeholders such as internet service providers, applications developers, and administration can be of utmost significance. This study integrates the results from literature review, international efforts, case study results, and qualitative analysis and proposes a Child Online Safety framework in India. The inferences contributed in this study titled **"Child Online Safety: A Select Study in Indian Context"** can be vital for the allied stakeholders making or inculcating optimal preventive measures for constructive internet usages in children.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES and FORMULAE

LIST OF ABBREVIATION

ACMA	Australian Communications and Media Authority
AVE	Average Variance Extracted
BIK	Better Internet for Kids
CCI	Commonwealth cybercrime Initiative
CDAC	Centre For Development of Advanced Computing
CEOP	Child Exploitation and Protection Centre
CFA	Confirmatory factor Analysis
CNN LSTM	Convolutional Neural Networks Long Term Short Memory
COP	Child Online Protection
COPPA	Children's Online Privacy Protection Act
COS	Child Online Safety
CTO	Commonwealth Telecommunications Organization
EU	European Union
FBI	Federal Bureau of Investigation
ICT	Information and Communication Technology
Interpol	International Criminal Police Organization
ISEA	Information Security education and Awareness
ISP	Internet Service Provider
ISTTF	Internet Safety Technical Task force
ITU	International Telecommunication Union
IWF	Internet Watch Foundation
LEA	Law Enforcement Agency
OSTWG	Online Safety and Technology Working Group
MASE	Multi-Agency Sexual Exploitation
MASH	Multi-Agency Safeguarding Hub
MEITY	Ministry of Electronics and Information Technology
NCAB	National Centre Agist Cyber Bullying
ROI	Region of Interest
RNN	Recurrent Neural Networks
SEM	Structural Equation Modelling

SNS	Social Networking Sites
SPSS	Statistical Package for Social Sciences
SVM	Support Vector Machines
TFIDF	Term Frequency Inverse Document Frequency
UNICEF	United Nation’s Children Fund
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNODC	United Nations Office on drugs and Crime
VGTF	Virtual Global Task Force
YPRT	European Youth Protection RoundTable

PUBLICATIONS BASED ON THESIS

1. Dittin Andrews & Sreejith Alathur (2018). E Discovery Tools a Benchmark Survey- IETE International Conference on Big Data Analytics.
2. Andrews, D., Alathur, S., & Chetty, N. (2020). International Efforts for Children Online Safety: A Survey. *International Journal of Web Based Communities*, *16*(2), 123-133.
3. Andrews, D., Alathur, S., Chetty, N., & Kumar, V. (2020, October). Child Online Safety in Indian Context. In *2020 5th International Conference on Computing, Communication and Security (ICCCS)* (pp. 1-4). IEEE.
4. Andrews, D., Alathur, S., & Chetty, N. (2020, December). Child Online Safety Intervention Through Empowering Parents and Technical Experts: Indian Context. In *International Working Conference on Transfer and Diffusion of IT* (pp. 662-673). Springer, Cham.

CHAPTER 1

I N T R O D U C T I O N

1.1. Background

The rapid growth of information technology and allied applications has widened the horizon for human beings to fulfill personalized demands. Internet technology is one of the most sought and inevitable inventions in the human era, increasing exponentially to serve different industries and purposes, including business, research, education, defense, and science (Internet World Stats, 2021). Internet usage for the general public has always been made for daily decision-making, education, communication, and socialization purposes (Livingstone and Haddon, 2009). However, in the last few years, internet use in youngsters below 18 has increased exponentially. Numerous purposes such as education demands, web-content access, and electronic conversation have been the dominant reason given behind Internet usages by children. The Internet has vital significance towards children's purposes, such as educational requirements, extra-knowledge, exploratory intends, entertainment (Holloway et al., 2013); however, it has resulted in adverse results in the last few years (Valentine, 2004). Internet does have a positive role for children by enabling them communicating with peers, friends, family members; the possibilities of getting in contact with malicious users or ill- web content cannot be ignored (Holloway et al., 2013). Such contacts might lead to mental disorders; misguided social behavior and self-destruction (Park, 2012; Richards et al., 2010). Researches reveal that majority of the parents encourage their child by enabling easy access to the internet, hypothesizing that they (children) use it for educational purposes or entertainment (Holloway et al., 2013). On the other hand, in current conditions, schools have been encouraging children to use computers and the internet to gain more information or knowledge by discovering educational electronic contents (Hopkins et al., 2013; Holloway et al., 2013; Daramola 2015). Social Networking and computer literacy have been given a broad reason being promoting the Internet for children (Collin et al., 2011; Hopkins et al., 2013; Holloway et al., 2013).

Recent studies reveal that children's regular use of the Internet often leads to unwanted contacts that invite "Stranger-danger," which eventually results in threat, child exploitation, grooming, and offline exploitation. Parents too are conscious about such events, though social affinity and flexibility limit them to prevent children from using the Internet (Ktoridou et al.,2012; Valentine, 2004). Restricting children from using the internet has been the dilemma for parents who believe that the child uses it for

educational or causal electronic communication purposes (Livingstone and Helsper, 2009; Jackson et al., 2003). In such cases, there is an inevitable need to design a specific robust mechanism to avoid scopes for child exploitation while facilitating children with Internet connectivity (Livingstone & Helsper, 2009). Stranger-danger caused due to Internet has given rise to numerous issues, including online bullying (Shahidullah and Shahid, 2017)). The Internet enables bullying to take place undisclosed. Though the evidence of bullying has been found online and offline, online activities have broadened the root cause for significant cases (Millwood Hargrave and Livingstone, 2007). Internet is extensively unregulated due to business-centric culture, ill-treated government policies, ill-intended intruding efforts, and malicious data sharing (Safenetwork.org.uk, 2014.). In the last few years, due to ease of access to the internet technologies, pornography has increased significantly, causing objectionable materials exchange, sharing across peers, though known or unknown. It had become a significant root cause for online child exploitation (Millwood Hargrave and Livingstone, 2007). Studies reveal that a very significantly small fraction of children have seen such materials as they dislike it; however, it has reached a significant population in the last few years. It signifies that such contents have a different perception from the community, including children, which triggers it to grow, though it has long-term devastating consequences (Millwood and Livingstone, 2007). Studies reveal that people who are excessively addicted to the internet are prone to be solicited and get in contact with the wrong person or communities (Mitchell et al., 2001). It was found that a significant fraction of children using the internet regularly undergoes awful and unwanted situations that eventually impact their education, health, and social behavior (Mitchell et al., 2001). Such facts alarm the community to explore preventive measures. Generalizing a solution is a global challenge. Online child exploitation has surfaced globally in different forms, including online exploitation, harassing and offline grooming, and sexual harassment (Cooper, 2002; Sawmy, 2013). The risks observed in recent years are like pornography, bullying, receiving sexual messages, sexting, strange contacts causing blackmailing, sexual-favor seeking (Livingstone et al., 2010; Livingstone et al., 2011; Livingstone and Haddon, 2012).

The study reveals that cyberbullying, exploitation, and harassment has emerged due to different adoption strategies by ill-intended users or offenders. Studies also reveal that

online contacts and grooming create a mutual trust environment and relationship, which later turns into sexual contact followed by ill-intended exploitation (O'Connell, 2003; Davidson et al., 2016). Similarly, abusive material sharing too results in a socially weaker personality which eventually degrades the children's behavior. Web-cam-based communication has been found a prime reason behind blackmailing and exploitation. Sexting, audio, video communication with objectionable content on intend lead children trapped in online child exploitation. Blocking unwanted content has always been the classical suggestion to prevent children from contacting ill-posed strange contact or web content. However, contemporarily, children make numerous approaches to get access to such content. Though numerous efforts have been made to avoid such events, those are not sufficient to alleviate current conditions (Beckett, 2011; Child Exploitation and Online Protection Centre, 2011; Berelowitz et al. 2012; Gohir, 2013; Melrose, 2013; Research in Practice and University of Greenwich, 2015; Coy et al., 2016). Online child exploitation has turned into different social devastating conditions impacting children whole life, making them depressed, homeless, going-missing, gang-association, crimes (Harris and Robinson, 2007; Coy, 2009; Jago et al. 2011; Beckett et al. 2013; Smeaton, 2013; Klatt et al. 2014; Franklin et al., 2015; Brown et al. 2016; Coy et al.,2017). It is inevitable to prohibit cybercrimes by predictor identification, localization, and isolation (Modecki et al., 2014; Zych et al., 2015). Recently, a few pieces of research have been done towards assessing online offender behavior and children's experience due to online exploitation or harassment (Whittle et al., 2014; Webster et al., 2016; Livingstone et al., 2017, Collings, 2020). Such crimes are deep routed due to excessive addiction to the internet, sexual contacts, sexting, and pornography (Palmer, 2015; Seto, 2016). Identifying the gaps and investigating the developments in Internet filtering techniques (Livingstone 2010, Dowdell, E. B. 2013)and a series of safety actions for protecting children accessing rich content on the Internet can be vital to prohibit online child exploitation (Livingstone S, 2014). The study focuses on research techniques for mitigating online safety and security risks internationally. Currently, parental control software tools are used widely, which provides facilities to manage age-inappropriate content (Dowdell, E. B. 2013, Livingstone. S 2014). In addition to this, network-level blocking of content restricts access to child abuse material at the ISP level along with police or child care charity

organizations (O'Neill B, 2014; ITU, 2009). Analyzers used as a mechanism for data set creation (Stevanovic et al. 2013) related to various security attacks will be studied to identify training data sets for age-inappropriate content.

In this chapter, some critical research variables, including Information and Communication Technologies, different forms and nature of online child exploitation, different measures, and allied challenges, are discussed. Before discussing the overall research, methodologies, and allied analytical activities, briefing the research and allied research variables can be of great relevance. Summarily, this chapter can be stated as an introductory of the at-hand study. The critical research artifacts are discussed optimally to convey the research problem, at-hand conditions, measures, and possible future enhancement measures or solutions. The details of the above-stated artifacts are given in the subsequent sections.

1.2. ICT and Online Risks

Information and Communication Technology (ICT) have brought benefits to the users of every age around the world with the increase in the availability of rich content over the Internet (Soumitra et al., 2012) and is transforming societies and economies around the world (Ali et al., 2011; Stern et al., 2009; Andrews D et al., 2020). This technological revolution has also attracted children to benefit the most from it. There is a growth in the last two decades in accessing computers and the internet among young people. Likely to have extensive use, including social networking (Stephen et al., 2015), playing video games (Bryan G et al., 2008), and watching video sharing sites (UNICEF, 2012; Anja et al.,2015; Andrews D et al.,2020). In the current era of ICT, where the Internet is widespread, children are not covered with a shield against overt sexual material, emotionally intense content, and elements including images or videos which are age-inappropriate. Sharing personal information and information about families has happened willingly in a mutual expression of free online services (AIFS, 2015). It happens due to the lack of factual information about various attacks, threats that are identified as the source of danger, and exploitations (CEOP 2013) that are driving the predators to target the most vulnerable user base, children (Ribble, 2011; Allyson, 2012; Andrews D et al.,2020).

Internet is more and more getting a part of life, especially for children and youth. The potential is identified and exploited for communication, including social networking,

entertainment, online gaming, and academic activities, including information gathering (UNICEF, 2012). Internet is a constant and familiar presence through computing devices, mobile, and other communication technologies (Michael C,2015). The gap between offline and online is getting reduced daily, and segregation is becoming meaningless. Global reach, along with anonymous nature, is illegal upbringing activities growing exponentially, targeting children. (Stanley, 2011). Online pedophile networks are thriving, and sexual offenders are effectively exploiting the internet for child exploitation. Convicts are widely using the internet for disseminating pornographic images, videos, and textual stories in the form of blogs (Bryce et al., 2011; Andrews D et al., 2020). Additionally, pedophiles use social networking sites, newsgroups, and chat rooms to deceive themselves as children for sexual communication (Wolak et al., 2008).

Online child safety is a global issue and requires a global response. Many countries have taken steps to battle with it by introducing online child safety or protection-related acts and initiated various awareness programs (Livingstone et al., 2014; Isaac et al. 2014; ITU, 2015; UNICEF 2012; Andrews et al., 2020; Andrews D et al., 2020). The preparation of standards and guidelines for children or young people, parents, caretakers, pedagogues, policymakers, and industry is taken up by few international research organizations (O'Connell, 2003; ITU 2015, Andrews et al.,2020).

When it comes to the growing number of Internet users, especially children, India is not much behind other developed nations (IAMAI 2015). Hence, foreseeing the need for online child safety, the Govt. of India has taken the initiative towards formulating a separate sub-section (section 67 B) on online child safety in its Indian IT Act 2000 and Indian IT Act Amendment 2008 (IAMAI 2015, Indian IT Act 2000, Indian IT Act Amendment 2008). There is much more left to be done in India to ensure the complete safety of teenagers.

The study focuses on research techniques for mitigating online security risks. From the above discussion, the primary focus is to investigate the developments in technological developments (Livingstone et al. 2010; Dowdell, 2013) and a series of actions for children's safety while accessing the content on the internet (Livingstone S, 2014). Some of the vital research parameters such as online risks, the topology of online risks, policy measures to protect children online are discussed in the following subsections.

It is a significantly challenging task to provide the definition or summary of the concept of online risk. It is necessary to understand the relationship between the risk categories, including exposure to content inappropriate for children and privacy risks. Noticeably, concerning the definitions of risk stated in literature and documents, a shared understanding of various risk categories is discussed in this research. However, for this research, some critical online risks for children are discussed.

1.3. Assessing Online Risks

Undeniably, there exists more non-uniformity regarding verification and proof for online risk(s). The frequency with which children unexpectedly face or experiences something hostile like online exploitation, pornographic offenses, bullying, contact by unknown persons cannot be quantified straightforwardly, which leads to ethical and measurement questions (Livingstone S et al., 2017).

1.4. Typology of Online Risks

The broad spectrum of children's use of the Internet is reflected because of risks to children online. International Telecommunications Union (ITU) Policy Makers guidelines of Child Online Protection, the European Youth Protection Roundtable Toolkit (YPRT), EU Kids Online, the Australian Communications and Media Authority (ACMA), the US Online Safety and Technology Working Group (OSTWG), and the US Internet Safety Technical Task Force (ISTTF) have contributed to the categorization of online risks. At the same time as above, mentioned classifications reflect the associated method considered by these studies. These classifications are well discriminated in between risks on damaging content those to related unfavorable interactions. On the contrary, the criteria of other categorizations can vary accordingly. Additional criteria for risk categorization include child interaction with a machine or human leading to the collection of personal data, cyber grooming and cyberbullying, illegal downloading leading to exposure to pornographic content, general online risks including malware and privacy (OECD,2012).

The degree of resilience or maturity and age can also be considered as critical criteria. Eventually, based on the criminal dimension, risks can be differentiated: those for which the child commits a criminal offense, those for which the child is a potential

victim of a criminal offense committed by a third party, and those that do not have a criminal dimension.

1.5. Internet Technology Risks

The growth of the internet and online social networks has paved the way for numerous security risks. Risks include privacy risks(Boshmaf et al., 2011; Mislove et al., 2010), sexual harassment(Wolak et al., 2008), identity theft (Bilge et al., 2009), malware(Baltazar, 2009), fake profiles referred to as Social bots(Boshmaf et al. 2011) (Elishar, 2012)and many more. Online social networks allow users for exposing private details, including the status of the relationship, sex, birth date, name of the school, email address, contact numbers, and physical location, which in turn can use in the virtual world as well as real-world for harming children (Boshmaf et al., 2011). Children are experiencing various threats targeting them. In the present era, children face threats concerning personal information safety related to Internet pedophiles or online predators. Risks and harms map to various online activities, including harm from content, harm from contact, and harm from conduct (Hasebrink et al., 2012; Wolak et al., 2008). The second type of threat targeting children is related to risky online behaviors, including online communications with unknown persons, chat rooms for communicating with strangers, explicit sexual talk, and sharing photos and videos (Wolak et al., 2008). Cyberbullying is the third type of threat targeting children. Bullying uses various communication platforms, including email, chats, online social media, and mobile conversations. Attackers harass the victims by sending hurting messages, sexual remarks, publishing images and videos which may be embarrassing, and engage in any other inappropriate activity(CRC, 2016; Mishna et al., 2009).

Nowadays, children are growing up along with the Internet. Therefore, they are called "digital natives." Children are eager to use the internet whenever they get an opportunity. Noticeably, Interactivity is one of the essential characteristics of the network. Thus, applicable online threats to children encompass contact risks and content risks. A snippet of the content risks and contact risks is discussed below.

- **Content risks**

Content risks are categorized into:

i) harmful advice,

ii) harmful content or age-inappropriate, and

iii) illegal content.

According to the risks and various factors, the potential consequences will vary, for example, a child's age and resilience.

Harmful advice: Generally, it is more difficult to control such kind of content with harmful advice. Because it can be placed on Web 2.0 platforms by anyone, including children and minors, moreover, it is hard to recognize the helpful or harmless advice and harmful advice because data on this concept can be intentioned or mix well-intentioned with potentially harmful advice (Millwood Hargrave et al., 2009).

Age-inappropriate: In many countries, contents like pornography, violence, or hate are legal but ruins children's development. Unintentionally, Children can fall under age-inappropriate kind of content. Children can access the contents and be referred to it by peers. Children can connect to collective interactive media, including online video games, which characterizes violence. Generally, such contents are generated and available commercially or freely to Internet users. The accessible Internet material for the public community is frequently not responsive to the particular state of child audiences. Undeniably, the content that harms minors targets children through deceptive domain names.

Age-inappropriate content is prone to reflect societal values and regional or national. Traditional television regulation is focused on subjective discussion (Millwood Hargrave, 2009). The video and program content associated with sexual and pornography should be the public concern (De Haan and Livingstone, 2009). Pornographic and violent content is the most significant kind of age-inappropriate content. Considerable reviews of the evidence on the pervasiveness of risk and their penalty for children exposed to such kind of contents are obtainable in various countries (Media Awareness Network, 2005; Hasebrink et al., 2009; Dooley et al., 2009; ISTTF, 2008;)

Illegal content: Content that is unlawful to publish and varies across administrative boundaries. In some countries promoting, hate speech, racism, bestiality, and other forms of inequality are unlawful. However, in most countries, the content on children's sexual exploitation is illegal, even though the frequency of the content associated with children's sexual exploitation is not known or significantly less.

- **Contact Risks**

Generally, contact risks come into existence when children expose to the internet, especially when children performing online chats. In addition, contact risks can be classified based on:

i) intentional communication to harm the child (e.g., cyber-grooming),

ii) Exposure to despicable online interactions, or

iii) the child is imposing harm by his or her conduct (e.g., illegal filesharing).

Cyber-grooming: In most countries, the activities like internet use by an adult to get a positive relationship with a child using the internet, including sexual contact, are generally a criminal offense. The authenticity of cyber-grooming looks complicated. In order to engage the child affections, it may start with falsification of the actual age of the adults. Moreover, in many cases, it has been noticed that there is no deception of any type in the online or offline relationship at any stage; sometimes, it includes legal minors or young adults (Dooley et al., 2009). Noticeably, it does not reduce the adult's accountability who considers the advantage of childhood innocence. It represents a requirement for a highly difficult understanding of prevention or how to deal with such a condition.

Online Harassment: The most recurrent contact risk faced by children is online harassment. Online harassment starts from humiliation, embarrassment, and intimidation in order to provide harsh by electronic means. It can terminate in cyberbullying where repeated and deliberate use of communication technology or information by individuals or groups harms others (Dooley et al., 2009; De Haan and Livingstone, 2009; ENISA, 2007). However, cyberbullies and their victims are minors, and there exists a child's harassment by an adult. The strategy consists of frequent intimidation by publication, chat or text messages, e-mail on the web, or distribution of content causing embarrassment, generally having the advantage of the relative secrecy of the online content (Dooley et al., 2009; ISTTF, 2008). Sometimes children have more interest and aggressive arguments through e-mail or instant messaging, referred to as flaming, cyberbullying, wherein children are victims and aggressors of such interaction. "Cyberstalking" is another kind of online harassment where an individual performs several kinds of online searches, including repetitive contact and malicious

intimidation. To cause physical or psychological distress, he/she may trade off the personal data of the victims.

Cyberbullying and online harassment look to be increasing concerns towards online child protection (Dooley et al., 2009; Wolak et al., 2007; Cross et al., 2009). The occurrence of cyberbullying varies significantly. Interestingly, older children are facing more risk. There is a correlation between the accessibility of electronic devices, including mobiles, and the distribution of online content access among youth(Hasebrink et al., (2009)). Considering the prevalence of risk, it is not possible to evaluate prevalence rates of the maximum amount of data. It is because cyberbullying can be defined that power imbalance and repetition between the bullied and bully, intent to harm, basically a kind of harassment includes aggressiveness, make use of communication technologies and information to bullying (Finkelhor et al., 2010; ISTTF, 2008)

Children share problematic information or online content leading to content risk; for example, they use a camera phone or webcam to share or post contents online (ISTTF, 2008). Unknowingly, minors forward their nude or seminude photographs, this kind of activity belongs to "sexting" and self-inflicted violence or images or videos portraying a group. It becomes harmful or illegal content and creates more risk when posted in the public domain, leading to long-term and short-term damage to the child's privacy.

1.6. Children Earmarked as Online Consumers

Children are facing risks online when

i) creating an economic risk (e.g., online frauds) being a vulnerable digital community
ii) exposure to advertisements related to products or services intended only for adults, including dating services
iii) online marketing messages of age-restricted products

- **Online marketing to children**

Online Marketing or advertisement can hurt minors with inappropriate content of age to which children can be exposed through banners or spam e-mails containing sexually explicit images. By promoting dating services, gambling, pornographic content, a minor's curiosity can get triggered and can foster risky behavior that might

eventually cause monetary loss or setting of the scene for sexual solicitation. Online marketing of harmful or age-restricted products increases concerns that such advertisements downplay risky lifestyles and link children to online suppliers. (Dooley et al., 2009). Generally, adolescents get primary risk due to promoting and selling illegal products like doping substances and drugs online (US Department of Justice, 2002). Online advertisements target children when there is no distinction between advertisement and content.

Moreover, put children at risk. Commercial contents are less distinguishable from other content for minors significantly younger children. It puts them highly vulnerable to the influence of online marketing (OECD, 2010b). An example of a marketing method is "Advergaming," which includes advertisement with online video or games (Kaiser Family Foundation, 2006).

- **Overspending**

Nowadays, most minors are overspending with mobile or online services that can become costly for parents (OECD, 2006). For example, when children can access online services only based on the fee structure or have the right to use online services through payment, they expend money to access it. Generally, most of the admirable online playing games require a subscription, and to access it; the players can significantly deserve actual costs for special virtual characters or virtual goods. There is a lack of appropriate data; hence it is difficult to recognize the amount of the problem.

1.7. Security Risks and Information Privacy

Security risks and information privacy significantly exists for all users. Generally, children belong to the highly susceptible group of online users due to the children's lack of awareness and less capacity to predict the probable consequences. For example, exposing personal data online can significantly create accessibility universally. However, there are inadequate safeguard measures to protect online security and privacy.

- *Children's Information Privacy*

Children suffer risks related to information privacy unknowingly when personal data is gathered through online modes automatically like cookies or when they fill personal information in online forms, upon request by third parties or service providers while

signing up for a service, or voluntarily. Like adults, most children are not interested in reading privacy statements in online services and agreeing to the terms. However, they face difficulty in understanding content written in a language. Ironically, children eagerly agree to use their data to get access to desired websites or online content. Personal information collected through various entities is transformed into an Internet commodity that applies to children and adults. It is significant to consider the fact that knowingly or unknowingly, children disclose information. Disclosed information can range from sharing personal data with a contact list to disclosing personal data to the entire online world. Children's attitudes towards privacy differ based on various factors, including age and individual preferences influenced by parental guidance. Even personal details of the children are posted or shared by another person (Marwick et al., 2010). For example, connecting individuals to their digital events, location, and photos are known as tagging. Nowadays, most minors are highly participating in this activity without getting authorization from individuals (ENISA, 2007). Sometimes, with malicious intent, a third party can use the personal data linked to individual profiles by minors. Noticeably, as compared to offline, children require security and privacy online.

Information Security Risks

An Internet user faces significant challenges towards information security. According to OSTW (2010), most children are predominantly vulnerable to online risks like information security, which significantly stem from malicious code like spyware and malware. Children lack any awareness regarding the risk and services that eventually land them into malware-caused or ill-intended risk.

1.8. Policy Measures to Protect Children

The various online risks for children are analyzed in the previous section. The current Section discusses existing policies to protect children online. Further, the section highlights differentiation in approaches and possible methodologies to reduce gaps and improve international cooperation. Further, this section discusses the key three dimensions of policies for protecting children online and compares the significant characteristics of different national policies.

Dimensions towards Policies

Different policy issues are raised depending on children's exposure to different kinds of risks. National-level policies for protecting children online are complex. The different dimensions of child protection policy are:

i) policy tools leading to multi-layered policies

ii) multi-stakeholder involvement policies depending on ownership roles and duties of stakeholders, and

iii) multi-level policies are covering national and international levels.

A snippet of three dimensions of policies is given in the following subsections.

Multi-Layered Policies

According to public policy concerns, online child safety has become a recent area. Noticeably, most countries are developing different policies to preserve children's rights, safeguard online internet usage by re-assessment of current policies, and developing new policy responses. Interestingly, methods being developed by all the countries include child safety zones, positive content provision, legislative, technical controls, regulatory controls, information security awareness, and educational programs. Extend to which nations are relying upon each of the policies are varying. There is a lack of evidencing for comparing the efficiency of high-level policies.

- *Legal Measures*

Noticeably, improving existing instruments has become more challenging for all countries than adopting supplementary laws and regulations. Countries agree that illegal offline is illegal online and is becoming a baseline criterion for online child protection. Most global societies and allied agencies understand that the Internet has outpaced normative concepts and legal definitions. If legal patch-ups emphasize too intently a precise use of technology, then they can become outdated quickly.

- *Self- and Co-Regulation*

Researches reveal that Self- and co-regulation can be the measure to avoid online child exploitation. Based on the communication freedoms and fundamental rights, self-regulation methods must be firmly reliable and optimistically decided. It is significant to update voluntary commitments for the particular situation to stay with advanced technology and social trends (ITU, 2009a; ITU, 2009b).

- *Technical Measures*

Noticeably, governments identify that a "silver bullet" solution is not available. Each of the methods has its advantage and disadvantage and should be applied in the most appropriate circumstances. Recently, the existing literature on online child protection identifies progress towards child online activity protection through "cautious optimism" and allied conscious-based use-decision (ISTTF, 2008). Some technology-driven methods like content labeling frameworks and report abuse functions reveal the advantage of technical measures towards risk mitigation and online safety improvement for the child. Interestingly, future efforts should endeavor to develop interoperability towards various distribution platforms and devices rather than enhancing the technology's usability, reliability, and performance (ISTTF, 2008; US FCC, 2009).

- *Provisioning Positive Content and Safety Zones for children*

Compared to other internet services, it is challenging to provide positive online content for children. Noticeably, few countries and EU members consider that protecting children online includes making the online experience positive. In addition, few countries ensure positive online content requirements, sometimes publicly funded and carried by assigning to public service media (e.g., in many European countries).

- *Awareness Inculcation and Education*

Awareness-raising or inculcation and education are the fundamental approaches globally to educate children about the content use, rights, grievances, and seamless communication. Additionally, people must be educated towards the vital policy tools that can help empower children. Effective awareness programs help children address the opportunities and risks and help promote the mitigation of children's risks online. (Livingstone and Haddon, 2009).

Multi-stakeholder effort

Identification of stakeholders, their role, and participation is essential in child protection policies.

- *Governments*

Choosing and following policy directions at the government level extends visibility to leadership commitment to protect children online, engage stakeholders at different levels, and facilitate coordination of efforts. Countries have taken up and discussed online child protection issues at the government level. Many policies have been

inculcated in India in the last few years to preserve child rights, and strict provision towards mistreatment with children is proposed.

Legal provisions related to Internet privacy are defined in the IT Act 2000 and the 2008 Amendment. The IT Act has provisioned for options that may safeguard online privacy in some cases, where in other cases, it dilutes online privacy. Penalizing child pornography and penalizing hacking and fraud and data protection standards are provisioned clearly in the IT Act. Privacy protection of the user is provided under IT Act. It comprises penalization for child pornography under IT Act Section 67(Mohanty 2011); penalization for hacking and fraud defined under IT Act sections 43, 66, and 66F (Mohanty, 2011); and definition of data protection standards identified for the body corporate (MCIT 2011). Provisioned acts for user privacy are diluted while user data is stored by a body corporate (MCIT, 2011), continuous collection and observing traffic data on the internet (MCIT, 2009) and real-time data analysis and continuous monitoring, prevention, and decryption of communications happening online (MCIT, 2009).

- *Children*

Vulnerable citizen children differ in age, degree of vulnerability, and resilience. Policies protecting children online must be tailored to their needs associated risks.

- *Parents and Caregivers*

Major societies across the globe acknowledge that Parents and caregivers play a crucial role in children's education. The role of parents is vital where governments are taking minimal responsibilities in regulating content and online activities. Parents are adopting various means in assisting children and mitigating online risks through timely guidance and technology adoption.

- *Educators and Public Institutions*

Educators are acknowledged for ensuring Internet usage ethics and online literacy while using online public online forums, schools, and libraries.

- *Private Sector*

The role of the private sector is widely recognized in protecting children online. Service providers are introducing nuanced safeguards and self-policing their information infrastructure platforms for protecting children.

Multi-Level Policies

Policies targeting protecting children online are developed at the national level, and the international level is in progress by inculcating fair and fit-to-all policy and operational collaboration. The elaborate discussion of the multi-level policies is given below.

- *National level*

Nations across the world have recognized their role in protecting children while using the Internet. Governments are developing national-level policies and directions aligned with Article 3 of the United Nations Convention regarding children's rights. Governmental level efforts help in driving and controlling involvement and issues with other stakeholders.

- *International Co-operation*

Typically, international co-operation has been considered significantly by the countries to protect children on an inherently global medium. International co-operation has formed many promising initiatives as a model other than sharing essential practices to protect children.

1.9. Research Gap and Motivation

With the rapid growth of the Internet in India and other developing nations, Internet governance organizations shall shape models of best practices including multiple stakeholders: children, parents, teachers, technologists including cybersecurity professionals, ISPs, non-government organizations, policymakers, governmental organizations, and LEAs.A national framework shall be introducing a novel way of defining the workforce responsible for retaining children safe in the online environment. The national framework shall also motivate establishing competency matrices or defined standards for those who contact children online, ensuring that they deliver a structured, accurate, and consistent set of policies and standards supporting children online (Hasebrink,2008).

Considering the possible preventive measures, the study found that applying content filtering, blocking, multi-stakeholder-based inclusive content monitoring, and filtering can be vital to make the internet safe for children (Hubbard and Bygrave, 2009; DeNardis and Raymond, 2013; Kleinwächter, 2007). Though, an educational approach or cyber counseling can also be recommended (Beckett et al. 2013; Firmin, 2013; Berelowitz et al. 2014). Putting a cap over online gaming habits can also help to prohibit

children from coming in contact with unwanted ill-posed web content (Kummer, 2012). Parental control approaches have always been the dominant solution to avoid child exploitation and strange contacts online (NetNanny, 2019; Kummer, 2012). SMART E-safety can be a viable solution to avoid online child exploitation (Boshmaf et al., 2011; Mislove et al., 2010; Baltazar, 2009; Elishar, 2012). Monitoring online communication and identifying the peer can also avoid exploitation (Hasebrink et al.,2012; Wolak et al., 2008). Observing social media open chats, abusive languages, communication patterns, social-behavior, sexual remarks, publishing images, and content sharing types can be considered by parents to identify a child under any threat and even help avoid exploitation probability (CRC 2016; Mishna et al., 2009).

Researches have been done to identify child exploitation, allied issues, and causes; however, the majority of the studies are done for European Nations or Western countries. No significant researches surfaced for the Indian scenario. On the other hand, no significant study could amalgamate perception and suggestions from the different stakeholders to make an optimal and optimistic inclusive approach to avoid online child exploitation. The research emphasizes understanding the contemporary conditions of online child exploitation, causes, and risk mitigation measures to design a novel inclusive preventive solution. The technological growth is driving the predators to target the most vulnerable user base, children. Online child safety is identified as a global issue. Lab setup provides a survey of various commercial and open-source electronic discovery applications, which shall cater to the identification of age-inappropriate contents. The study provides a comparative analysis of the standard and unique technological features of various solutions. This study follows a Mixed Research Paradigm. Different stakeholders, including children, parents, technical and legal experts, have been interviewed to understand contemporary online (internet) use patterns, purposes, threats, child exploitation conditions, and possible optimal solutions.

1.10. Problem Statement and Research Questions

Undeniably, the internet has become an inseparable part of people of almost all ages, each having its region of interest. While some access online sites and data for knowledge the others access it for entertainment. Noticeably, children nowadays also access online content for educational purposes, and it cannot be denied that the internet

brings lots of opportunities to children. However, it is also noteworthy that exploitation of the internet by children exposes them to new risks and dangers. The exponential rise in internet usage by children for different purposes, including academic, gaming, and social media surfing, has broadened the horizon for intruders or malicious entities to gain a particular point of contact with children that in later stage results in exploitation. Such exploitation can be of different forms, such as mental harassment, sexual exploitation, cyber-crimes, and ill-behaved activities. Such online cyber-crime activities might lead to disastrous consequences causing even loss of life and money. Different web-content filtering approaches have been developed; however, their efficacy to avoid cyber-crime described above or allied online child exploitation has not yet been studied and verified, at least in the Indian scenario.

On the other hand, different factors can, directly and indirectly, impact the success of any filtering approach. Behavioral aspects, perceptual aspects, preferences, and supervision, these types of factors can be there which might confine or promote the success and failure of online content filtering or parental control to avoid online child exploitation. Meanwhile, different stakeholders have different perceptions, such as children, parents, school teachers or authorities, lawyers, and technical experts, towards child's online search behavior, content filtering, use patterns, and risk assessment. It is crucial to assess the perception of the different stakeholders towards online child behavior, online child exploitation, and allied risks and potential solutions. In this research, the predominant emphasis has been made on assessing the perception of the different stakeholders towards child's online internet surfing behavior, child exploitation risks and alleviating measures, legal issues on content filtering, and probable optimal technical enhancement to prevent online child exploitation using advanced content filtering and multi-channel supervision and coordination systems. To achieve this, in this research, a mixed research paradigm including both qualitative and quantitative methods have been considered where primary and secondary data sources are considered to assess different stakeholder's perceptions towards issues as mentioned earlier. Being an empirical study, responses from different stakeholders, including children, parents, teachers, technical experts, legal experts, have been obtained, which has been examined analytically to understand the root cause of online child exploitation, preventive measures, and a conceptual model to alleviate at hand issues. This research

contributes a novel conceptual model to safeguard child's online search environment to make constructive internet source provision.

Research Question

1. How to improve child online safety in the Indian Context?

1.11. Research Objectives

In the last few years, escalation in the exploitation of the internet by people of different age groups has forced the allied authorities and industries to restrict some websites or some user-specific content to confine the cybercrime. It is noteworthy that there are now specially developed numerous techniques to prevent the exploitation of children who visit online websites and provide their details while logging on to any website. Hence, the principal goal of this research or study is to assess (empirically) internet security techniques to safeguard the users and their data from being misused. Undeniably, the internet has become an inseparable part of almost all ages, with each one having its region of interest. While some access online sites and data for knowledge the others access it for entertainment. Children nowadays also access online content for educational purposes, and it cannot be denied that the internet brings lots of opportunities to children. However, it is also noteworthy that children's exploitation of the internet exposes them to new risks and dangers. Hence, this research aims to prevent children from risks encountered while accessing online content since online child exploitation has been a concern across the globe. Children are more prone to face the risks associated with cyber-crime and finally end up harming themselves or their people. In this research, several constructs associated with facilitating safe online content access for children have been examined. It has been ensured that the study discusses and provides information about all the aspects allied with mitigation of cyber-crime, focusing on protecting children from the harm caused due to cybercrime.

To conclude, it can be asserted that the current study titled **"Child Online Safety: A Select Study in Indian Context"** emphasizes assessing online child exploitation and causative factors, risk mitigation frameworks, internet filtering schemes for online child exploitation avoidance. Considering this as a novel intend towards the issues and risks allied with cyber-crime, the key research objectives of this study are enumerated as follows:

1. To examine the distinctive issues pertinent to online child safety and protection

2. To analyze the adult content identification mechanisms based on E-discovery techniques.
3. To explore the existing global practices addressing Child online safety
4. To study and examine a risk mitigation framework addressing children's online issues in the Indian Context

1.12. Structure of the Thesis

Considering the optimal thesis presentation requirements, the overall contents have been divided into seven individual chapters in this thesis. The overall thesis outlines defined are given as follows:

Chapter-1 Introduction

This chapter primarily discusses the introduction of the proposed research work or thesis. Primarily, key research variables such as online child risks, the topology of online risks, and policy measures to protect children online are discussed in this chapter. In addition, the critical research introductory containing research objectives, proposed research, problem formulation, and thesis outline are also discussed in this chapter. The key benefit of this chapter is to provide sufficient knowledge transfer for the at-hand research and allied activities.

Chapter-2 Literature Survey

In this chapter, primarily, the critical works of literature about the online risks for children and policies issues and available solutions for Online Child Exploitation and Internet Filtering Techniques and policies to protect them as Internet users are discussed. Also, the chapter discusses the International Efforts for addressing Child Online Safety issues.

Chapter-3 Research Design

The chapter predominantly discusses the research design and the snippet of fundamental methodological paradigms based on the research questions and objectives. This study can be stated as a behavioral assessment paradigm where the respective perception of the allied stakeholders has been assessed to identify critical factors that impact the techniques and decisions to prevent online child exploitation. This study encompasses a mixed research paradigm that uses both qualitative as well as quantitative research methods. Realizing the significance of the different stakeholders such as children, parents, tech-experts and legal experts who can help to identify

different psychological traits signifying online harassment symptoms, behavioral changes, online surfing behavior, causes of exploitation, need and optimal model of inline internet usage and different preventive measures to avoid child (online) exploitation, the chapter discusses the qualitative as well as quantitative methodologies employed

Chapter- 4 Case study

Chapter 4 addresses three case studies in detail: (i) A Lab setup that provides test results of various commercial and open-source electronic discovery applications, which shall cater to the identification of age-inappropriate contents. (ii) Analysis of online social media responses and awareness posts on children's online safety (iii)Study on cyberbullying detection in social media text messages.

Chapter-5 Stake Holder Survey and Analysis

This chapter primarily discusses the data analysis and allied inferences. Being multi-stakeholder research, the chapter provides the analysis for each stakeholder -Children, Parents, Technical experts, and Legal experts. The analysis is performed distinctly in terms of demographic as well as descriptive components. The synthesis of the stakeholder survey is explained in the chapter. A predictive analysis of parents' and technical experts' opinions is performed to test some of the chapter's hypotheses. Based on the identified variables, the different hypotheses on predicting parent and technical experts-initiated child online safety have been set in Chapter 5.

Chapter:6 Design of Model for Child Online Safety using SEM

The chapter discusses the analysis of primary data and detailed interpretation of the results collected from technical experts. The chapter discusses developed models for Child Online Safety and testing using Structural Equation Modeling (SEM). The chapter also discusses the tests performed for testing the validity and reliability. The chapter provides the characteristics of the samples and describes a model for Online child safety. The vital analysis carried out before going for reliability and validity testing includes the tests for Quality of Primary data; Adequacy of sample size; Identification of missing values, and Identification of outliers. The chapter also includes a section for presenting the procedures used to test the measurement model's reliability and validity, including testing of convergent validity, discriminant validity, nomological validity, and face validity. The chapter provides Convergent validity,

Discriminant validity, Nomological validity, and Face validity and corresponding assessment by performing CFA/SEM for the latent constructs. The chapter provides the characteristics of the samples and describes the model for Online child safety.

Chapter-7 Synthesis and Conclusion

The overall research conclusion and respective significances are discussed in this section. In addition, the future scope has also been presented in this chapter of the presented thesis.

Reference

In this section, the references used in this research work and thesis preparation are presented.

1.13. Conclusion

The Chapter presents the preface for the current study. The chapter delivers a background of the study, its significance and preliminary literature review, motivation of the research, research gap, and research objectives. The overall structure of the thesis is given in the chapter. The next chapter discusses the critical literature on the online risks for children and policy issues. Also, the chapter discusses the International Efforts for addressing Child Online Safety issues.

CHAPTER 2

LITERATURE REVIEW

2.1. Introduction

The previous chapter introduced the background of the study. This chapter discusses the theoretical and empirical background and identification of research gaps that are structured as follows. The chapter provides a theoretical background of this study, reviews literature published, and discusses the international efforts for addressing Child Online Safety. Finally, this chapter ends with a conclusion.

2.2. Background

Internet security is making headlines. It is one of the live topics in the digital era. Modern technology is growing speedily in today's digital period. The internet has become an inevitable part of our lives. Using the internet brings lots of opportunities to children, but it also exposes them to new risks and dangers. Online Child Exploitation has been a concern across the globe. Children are more victims of exploitation than older people.

The developments such as educating adults (Rizo et al., 2019), strengthening legal provisions (Mantelero, 2016), and effort to protect from online risks (Schleicher, 2019) are flourishing in online communities. As commercial sexual exploitation is increased, it is time to educate youth about reducing the occurrence and impact of sexual exploitation (Rizo et al., 2019). Even though the Internet addiction prevention initiatives for adolescents are taking place at the school level are, the skill development and use of protective factors are essential to reduce the impacts of Internet addiction (Throuvala et al., 2019). As education takes a long time to act against the online risks, legal provisions are still effective for protecting children's rights and personal information online (Mantelero, 2016). Apart from ICT usage in education, reasonable efforts must be protected from bullying, phishing, and illegal content (Schleicher, 2019).

In online communities, anonymity plays an essential role in individual and group identities (Kim et al., 2019). As online communities are open environments, the formation of the norm is essential for the proper functioning of communities (Ivaturi and Chua, 2019). Global Kids Online is a new initiative that provides tools and guidance to the researcher related to online risks reduction (Byrne and Burton, 2017).

Communities of practice are professionals' network which assists in sharing knowledge online (Johnson et al., 2019).

With the advancements in ICT, online risks to children are increasing. To counter these increased online risks, it is essential to understand the ecosystem and collective effort. Therefore, this study attempts to present different forms of online risks to children, influencing factors to address online children's safety, and international efforts towards attaining online safety. To obtain information on literature, the Scopus and Google scholar sites are searched with the appropriate keywords as a part of the methodology. As stated, the current study emphasizes assessing online child exploitation, causative factors, risk mitigation frameworks, internet filtering schemes for online child exploitation avoidance in the Indian Context. Summarily, this study emphasizes studying and quantumly exploring the different at hand solutions, allied strengths, and limitations. Future scopes to alleviate online child exploitation events, which have increased significantly as per the high-pace increase in web technologies and internet-enabled services, are included in the current study. This thesis assesses both primary and secondary data as a mixed research paradigm-based study, where the latter enables identifying the research variables and allied discussion. The assessment of the different secondary data enables a researcher to understand the related subject matter, existing or hypothesized inferences, which eventually leads to defining customized hypothesis as research backbone or guiding structure. It is also vital to understand allied independent and the dependent variables, which guides overall research and allied methodologies. Considering it as motivation, the different literature on online child exploitation, causes, and resolution to avoid any destructive consequences is discussed in this chapter. Eventually, it is targeted to formulate a novel and robust conceptual model for risk mitigation strategy to avoid any online child exploitation possibility. This chapter briefs the critical literature about internet technologies, internet use patterns amongst children, online child exploitation cases, different topologies active online towards child grooming, and different initiatives made towards online child exploitation risk avoidance. Subsequent sections carry out an in-depth discussion on the aforesaid subject matters.

Undeniably, online child exploitation or allied risks comes into the picture only when considering internet technologies as the use pattern. However, it depends on the use

pattern. Since internet technologies have facilitated several contributions towards making the social-scientific or economic arena improved and augmented, its adverse effects can also be not neglected. Considering these factors, understanding Internet technologies, their application, and the allied vulnerable (virtual) world can be of paramount significance(Andrews D et al., 2020). With this motive, the following section briefs about Internet technology and Internet communication technologies.

2.2.1. Internet Technology and Potential Risks

The rapid development of internet technology has recently enabled or broadened the horizon for the different possibilities serving a significantly ample application space and allied demands. Internet is considered one of the most used and revitalizing innovations in human society, which has greatly benefitted the world. Nowadays, the active use of the internet in almost every aspect of life by people and corporate has been enabled because of significant benefits and services provided via internet facilities (Livingstone, S. M.and Haddon, L., 2009). The bandwidth of the internet has been gradually enhancing and becoming global spread. Currently, approximately 65.6% of the whole world population is having access to the internet. A growth of 1331.9% Internet penetration happened during the last two decades. Noticeably, there was an increase of only less than 1% of internet users worldwide two decades ago (Internet World Stats, 2021). Interestingly, from 2001 to 2021, the number of internet users has been enhanced significantly tenfold (Internet World Stats, 2021). Internet technologies have given a broadened horizon for online activities, including both positive as well as harmful.

Internet is more and more getting a part of life, especially for children and youth. The potential is identified and exploited for communication, including social networking, entertainment, online gaming, and academic activities, including information gathering(UNICEF 2012). The Internet is a constant and familiar presence through computing devices, mobile, and other communication technologies (Michael Chan et al.,2015). The gap between offline and online is getting reduced day by day, and segregation is becoming meaningless. It is of paramount significance on the one hand, while inappropriate use might even impose adverse effects.

Global reach and anonymous nature are illegal upbringing activities growing exponentially, targeting children(Stanley, 2011). Online pedophile networks are

thriving. Sexual offenders are effectively exploiting the internet for child exploitation. Convicts are widely using the Internet for disseminating pornographic images, videos, and textual stories in the form of blogs(Westlake, B.G et al., 2011). Additionally, pedophiles use social networking sites, newsgroups, and chat rooms to deceive themselves as children for sexual communication(Wolak et al., 2008).

Considering the role of the internet for children, the demand towards online education, online classes, training, and numerous schools related assignment activities have become possible only because of the Internet facility. During the Covid-19 pandemic (2020-21), Internet technology emerged as a single possible solution to let education or allied activities reach children. Internet-based educational platforms are being widely employed during the Covid -19 pandemic(Kumar and Pande 2021). Many business enterprises have emerged in sync with such requirements that serve educational activities and allied materials online in the last few years. This fact indicates that internet technology has become near-inevitable for children in modern society, which is expected to increase in the future. Therefore, to ensure a seamless and healthier use environment ensuring content suitability is equally a must. Predominantly, cyber-crime avoidance measure is required to be ensured. The following sub-section provides a snippet of the different ways leading to online risk possibilities. Before discussing the different possibilities, a snippet of the online risk behavior is given in the subsequent section.

2.3. Online Risky Behavior and the Internet

Internet is providing opportunities to children. Although Internet can be used as the medium for their learning, self-articulation, and managing their association with friends, relatives, and peers, they often promote logical consequences related to age-appropriate content and privacy(Shin and Lwin, 2017)). ICT has intensified the potential of crimes traditional crimes involving the exploitation of children. Social networking platforms and online forums uncover traditional borders. Children are creating and using their virtual social platforms for networking. Potential abusers are sharing age-inappropriate materials with like-minded people. ICT has played a major role in creating a natural surrounding with easy access to pornographic content. Cyberbullying is relatively low risk from the bully perspective due to anonymity and lack of governance. Pedophiles are finding victims without leaving space to be caught

in the eyes of LEA. Approximately one-third of internet users are children accounts (Pūraitė & Prokof jeva, 2019). Risks including cyberbullying, contact establishment with strangers, sexting, and pornography affect children(Livingstone & Smith(2014). Most wrongdoers nowadays are complicating the LEAs with the help of storage devices that include robust in-built encryption techniques (Pūraitė & Prokofjeva, 2019).

2.3.1. Unwanted Contact

Unwanted contact is one of the risky areas for internet users. Interestingly, "stranger danger" is a significant focus of concern with the potential of daunting contact from unknown persons, predominantly pedophiles. Fear of the likelihood of children being abducted and subjected to cruel treatment by unknown strangers has increased drastically. Such anxious feelings regarding online access are required to be placed in the broader context of growing anxiousness about risks to children.

Noticeably, the government's use of police and law enforcement is impossible as the Internet is largely unregulated in content risk. However, cybercrime is universally acknowledged in different forms, including disrupting other internet users' activities by spreading malicious viruses. There is a requirement of moral guidelines to deal with such problems. Typically, in the world of metropolitans' streets, exposure to information or images is as caustic as anything accessible (Safenetwork, 2014). Further, it has been observed that the classical or at-hand efforts to understand the dilemma by controlling children's internet activities or limiting children's access to the internet, or either ignoring the risks or restricting their online opportunities are not that encouraging. Some researchers concluded that the children could face an additional risk for those who face different online experiences. Therefore, There is an inevitable need for additional solutions to address the contemporary online child exploitation problem(Livingstone &Helsper, (2009). Bullying is another different category of unwanted contact. It has been noticed that most of the children experienced online bullying(ECPAT, 2020). In addition, secret bullying is allowed by the internet, which also distributes more widely. However, it has been noticed that other than online, bullying takes place offline by the children (Millwood Hargrave and Livingstone2007). Also, there is an indication that the internet is leading to an increase in bullying. Noticeably, for further research, there exists a question of how online bullying might support new combinations of techniques and offline bullying.

2.3.2. Violence Offline

The internet can distribute material with pornography that encourages various kinds of violence. These materials may consist of hate sites, pornographic content, which result in encouraging different forms of self-harm. Noticeably, some of the pieces of literature depicted that few children have seen those kinds of materials. Some children dislike it, and generally, some of them are disturbing (Millwood Hargrave and Livingstone, 2007). There are significant, few discussions related to how children make sense of such material and its possible effects.

2.3.3. Consequence of Internet Usage by Young Children

Most children spent their time with online activities rather than interacting with family and friends and community activities. In general, other than emails and phones, the internet supports connecting family, friends, and others who are located geographically remote, employing various applications like WhatsApp, Viber, and skype. Towards young people who are getting hooked to the Internet is a concern about worldwide penetration growth. Addiction (towards the internet) is significantly studied and analyzed for a clinical condition to be treated. Furthermore, research also has been done on the use of pathological internet, which causing damage to people and can exist mental disorder trace, for example, depression (Park, 2012; Richards et al., 2010).

Positive Effects

Other than the noticeable entertainment, most children experience connecting with people online, watching videos, and engaging in online gaming. In addition, the trending digital literacies develop in children due to their interaction with the internet. Additionally, future academic accomplishments are also supported significantly by it, for example, social interaction wellbeing and data mining (Judge et al., 2006; Marsh, 2010; Johnson, 2010; Cavanaugh et al., 2004). Most parents believe that internet exposure allows children to determine pertinent information online hence increasing imagination and creativity. Very young children can explore imagination and acquire knowledge in secure and valuable methods.

Parents support their children's early access to the Internet to enable an opportunity to discover and play online and search the content of their education purpose(Holloway, Green & Livingstone (2013). In developing and developed countries, the majority of the children started their proper schooling years with considerable knowledge with the

use of the internet and computer technology. They indicate that the Internet is significant towards developing knowledge and skills in generating, retrieving, and traversing content (Siibak&Vinter, 2012; Edward Groves & Langley, 2009; Hopkins et al., 2013). Undeniably, various literacies are involved in the current digital age that disdains skills in generating, programming, understanding, and retrieving in different digital formats. The foundation has been produced to use these digital technologies' reactive use by those as mentioned above developing digital literalness skills. The effective use of the internet and computer technologies creates independent identity, supports self-expression and imagination, and entails good interpersonal associations. It is also vital to reinforce social networking and a sense of belongingness that eventually can contribute to digital social skills development (Collin, Richardson & Third, 2011; Holloway et al., 2013).

Adverse Effects

According to Cooper (2002), the internet has developed significantly with money making in sexually explicit material distribution and has become the channel for compulsive sexual behavior, sex crimes, and sex trafficking. Noticeably, using the internet, most children, about 90% ages between 8 to 16, have watched pornography movies or acts (London School of Economics, 2002). However, in many cases, by accident, the sex sites are retrieved by the child when performing homework for searching pictures or information through harmless words (Sawmy, 2013).

2.3.4. Impact of Cyber Crimes

The majority of the research towards Internet crimes has indicated illegal activities and the detection of various prevention methods for future activities. Moreover, some research also focused on measuring the psychological impact of these significant activities on children and the implication of related criminal activities. Concerning that, Cameron and Salazar(2015) found that both boys and girls aged 14 to 17 who use the internet regularly reported no sexually explicit material on their personal views of either relationship or gender. Authors have stated that only a minority of the college students stated that online pornography affects their sexual emotions and attitudes significantly when watching that before 18.

A peer-to-peer file-sharing network has been applied to perform the study on young people towards pornography. They state that sexualized material and pornography can

influence children and youth on their sexual violence, sexual attitudes, sexual activities, and moral values. In addition, the study of child molestation and pornography reported that pornography had been used by child molesters (individuals who commit sexual acts against children) to groom pedophiles (individuals whom children sexually arouse), where pedophiles are having a minimum interest in molesting children when viewing pornography. Eventually, the researchers stated that based on the number of risk factors, the person's behavior significantly affects virtual or accurate child contact. Hence, no significant effect or cause exists between committing sexual molestation of a child and viewing child pornography.

In sync with the above discussion, it can be inferred that undeniably online activities have a relationship with cyber-exploitation events. However, the internet use patterns of children and adults are different. With this motive, the following section briefs some of the critical literature discussing children's online activities and their results towards cyber-exploitation events.

2.4. Children's Online Activities

Nowadays, most young people and children are more likely to use the internet and digital technology and become an integral part of their lives. Generally, it can be observed that most of the children access various online activities in deep (Livingstone et al., 2012). Moreover, this thesis emphasized online risks towards children than advantages, so it is significant to realize the positive motivation of the children in using and choosing the internet. Therefore, that made to realize how children utilize the internet and how its costs for their well-being. Noticeably, when children exposed to online could face potential risks, they will not face them because of the nature of their activities. Both direct and indirect impacts have consisted in online risks. The online environment does not directly carry out this obesity problem, but the child's attachment to online causes a sedentary lifestyle that carries directly.

The use of the Internet by children consists of various fields, including socializing, entertainment, fun, education, and expressing themselves in various ways. Noticeably, most children engaged online with a wide range of different activities; most children benefit from these activities differently. Livingstone et al. (2011) observed that the majority of the European children performed their school projects using the internet. Ktoridou et al. (2012), on the other hand, reported that most parents are believed that

the internet consists significant positive effects on the advancement of children in school and their professional life preparation. Therefore parents encouraged their children to access the internet for educational purposes.

Indeed, there is a wide range of online risks available. Among the most critical risks include personal data misuse, the content generated by potentially harmful users, meeting online contacts offline, contacting people not known face-to-face, receiving sexual messages, bullying, and pornography (Livingstone et al., 2010). In addition to these, children are exposed to various risks; hence they become susceptible to various dangers. For example, children access the internet more for social activities consist messaging (Livingstone et al., 2011). There is frequent contact between Children and young people through social network sites, webcams, and instantaneous messengers. Disappointedly, such communication has negative impacts on children due to bullying and harmful messages. According to online research performed by the KU kids found that bullying spread risks among children significantly. Generally, bullying takes place online and offline as well. Noticeably, Livingstone et al., 2011) found that online bullying is little common, as stated by children. In addition, Livingstone et al. (2010) determined that cyberbullying is the most significant risk that upset young children the most but not that spread among them. Other than bullying, sexting is another risk factor related to messaging, and it has been found that it occurs more commonly in Finnish children in Europe (Haddon and Livingstone, 2012).

Generally, the risks mentioned earlier could be restricted and deal with only on the household level. Moreover, the technical solution can be implemented by parents such that they can restrict their children from accessing web pages, can monitor their usage. Moreover, it is necessary to realize that control of internet usage by children through different ways and places is more complicated. In addition, it also realizes that restricting children by accessing the internet is not a robust solution instead, keeping one's child safe on the Internet is the best solution. Nancy Willard (2012) provided details about 'cyber savvy' children having the required skills to navigate the online world. This idea is opposed to restrictive measures when parents and schools simply block access to unwanted content (Willard, 2012).

The above discussion states that children use the internet for various reasons, especially older children use the internet more widely than younger children (e.g., social

networking, uploading photos, homework. Childwise's (2017) affirmed that children aged 7-16 use the internet to upload videos, photos, and music (27%), look up information (38%), social networking (40%), interact with family and friends (47%), homework (47%), play games (54%), listen to music (56%), and watch video clips (59%).

2.4.1. Children's Internet Use

The majority of the research emphasized on risk and safety of children towards online use. Moreover, this section describes how the children are motivated and get expected benefits from utilizing the internet. In addition, the use of the internet highly depends on the children's gender, age, and socio-economic status (SES). Further, it is also based on the device, location, and frequency with which they access it. A detailed discussion of the use of the internet by children has been given in the subsequent section.

Children Internet Use in Virtual World

The majority of the children prefer the virtual world by accessing the internet. According to Holloway et al. (2013)," an increase in the number of children, especially pre-teenagers of age below 11 years, with access to virtual internet worlds is the most considerable enhancement with sharp growth". According to the statement given in the Young children (2011), "virtual worlds are the combination of the application of social network functions and application of games." Hence, it creates an online risk for children when they are accessible to the game-playing application.

According to the use pattern, children utilizes different kinds of Internet communication technology consisting:

- MySpace,
- Skype,
- Social network sites (Facebook, Instagram, Twitter)
- Instant messaging,
- Online games,
- E-mail,
- Chat rooms, and
- Blogs.

Since the current study mainly focuses on online child abuse or allied incidents to frame a novel preventive measure, discussing online child abuse and causative factors is vital. A snippet of the subject mentioned above matter is given as follows:

2.5. Online Child Abuse and Exploitation

According to Fox and Kalkan (2016), there can be an overlap between Online and offline exploitation(Fox and Kalkan, 2016). When there is an appearance of co-operation between children and young people, this could not be considered consent because they are legally minors and focus on various control and coercion forms. Generally, child exploitation is defined as "abuse where an individual or group takes advantage of an imbalance of power to coerce, manipulate or deceive a child or young person under the age of 18 into wrong activity" (New England definition,2017).

There is no one way CSE is perpetrated (Berelowitz et al.,2012; Research in Practice and University of Greenwich, 2015; Gohir, 2013; Child Exploitation and Online Protection Centre, 2011). Grooming exists in different forms of CSE, but not in every case(Beckett, 2011; Melrose, 2013). Sexual exploitation can significantly include peers in complex forms, including bystanders, abusers, or facilitators(Firmin, 2011). Most studies show only interest in young people between 12 to 15 years(Beckett et al., 2013). However, some research also concerns children aged between 8 to 11 years and observed an increased rate of online exploitation of children aged between 8 to 11 years (Department for Education, 2017). Noticeably there is no presence of a "typical" victim, and it indicates that few children are highly vulnerable to others. Indicator range highlighted that professionals must be alert that contains gang-association, running away/going missing, being in care, disability, misuse of substances, homelessness deprivation, and prior abuse in the family (Klatt et al., 2014; Harris and Robinson, 2007; Smeaton, 2013; Raws and Smeaton, 2015; Coy, 2009; Brown et al., 2016; Jago et al., 2011; Beckett et al., 2013).

2.6. Risk Factors of Online Child Abuse

The unprecedented growth of the online world has created anonymity and dispersion for law enforcement across the world (Hinduja and Patchin, 2008; Goodman and Brenner, 2002). Often, it is impossible to identify the physical location of the perpetrator of the crime committed through the Internet. Information sharing is a purpose of the Internet. The increased speed, ease to use, and the broader availability of networks made the sharing of millions of bytes of information or content in a short time. Intermediaries are the actors on the Internet and perform different activities such

as content uploading, hosting content, storing content, archiving content, cataloging content, and providing physical access to content as in Cyber Cafes (MacKinnon et al., 2015; House, 2009).

The Internet may be a part of life for children and youth and is potential for communication-social networking, entertainment- online gaming, and academic-information gathering (UNICEF, 2012). Access to the Internet is through computing devices, mobile, and other communication technologies (Chan, 2015). As the gap between offline and online activities is reducing gradually, segregating them is meaningless. Global reach with anonymous nature is increasing illegal activities and targeting children (Stanley, 2002). Online pedophile networks are growing, and sexual offenders are effectively exploiting the Internet for child exploitation. Exploiters are using the Internet for disseminating pornographic images, videos, and textual stories in the form of blogs (Westlake et al., 2011). Pedophiles often use social networking sites, newsgroups, and chat rooms to deceive themselves as children for sexual communication (Wolak et al., 2008).

With the online presence, children are facing different kinds of risks. Online risks to children can be classified as aggressive, sexual, values, and commercial (Livingstone et al., 2011). Aggressive risk involves violent content and can be used to harass children. Sexual risk is possible through pornographic content in the form of sexual abuse. Values risk involves hate content and can be exhibited based on identities. Advertising content is an example of commercial risks which can attack personal information.

Security risks and information privacy exists significantly for all users. Generally, children belong to the highly susceptible group of online users. It is due to the children's lack of awareness and less capacity to predict the probable consequences. For example, exposing personal data online can significantly create accessibility universally. However, inadequate safeguards are existing for the protection of their online security and privacy. Children face information privacy risks unknowingly when personal data are collected through online means automatically (e.g., cookies), while filling personal information in online forms, upon request by an information service provider while signing up for a service, or by voluntary means (YPRT, 2009). Generally, similar to adults, most children do not like to provide privacy statements in online services

(Fielder et al., 2007). However, they face difficulty understanding content written in a language (Fielder et al., 2007; Media Awareness Network, 2005). To get access to desired websites, children eagerly agree to the use of their data. Personal information is becoming an online commodity for adults and children. It is significant to consider the context, here children voluntarily disclose information. Disclosed information can range from personal data to the entire Internet to share personal data with friends.

Children's attitudes towards privacy differ. The difference is not only based on age but also on individual preferences, which can be positively influenced by parental directions and counseling (Marwick et al., 2010). Sometimes, personal details of the children can be posted or shared by another person. For example, connecting individuals to their digital events, location, and photos are known as tagging. Nowadays, most minors highly participated in this activity that children do not want and do not need authorization from persons (ENISA, 2007). Sometimes, with malicious intent, a third party can use the personal data linked to individual profiles by minors. Noticeably, as compared to offline, children require security and privacy online. The department of the library or school monitors a children's online behavior through a cyber safety strategy (Marwick et al., 2010).

An internet user faces significant challenges towards information security. It was found that most of the children are predominantly vulnerable to online risks like information security which are significantly stemming from malicious code, including spyware and malware(OSTW, 2010). Children do not have any awareness regarding the risk, and malware services result in higher risk. Beck (1992) affirmed that the "Nature of 'risk' facilitates complicated subjects to offer multiple meanings. It can wrap a pack of different facets and discussions".

Exposure to Harmful

This section describes the various pieces of literature pertaining to the children exposed to harmful due to the internet use in their daily activity. Sometimes children are knowingly or unknowingly expose to harmful when they access pornographic or other harmful content that judges to be harmful to their growth. Harmful content can include a wide range of images, video, audio, written content, or other material that can influence children negatively. The snippet of risk of harm to children online and classification and measure risk of harm has been given in this section.

Risk of Harm to Children Online

When children are accessing the internet for playing games applications like learning how to swim, bicycle riding, they create a risk of harm. Different conditions are assessed, signifying the risk factors, factors affecting risk and risks, and do not create physical harm(Livingstone, 2013). It indicates the presence of the policy risk that cannot eliminate risk but manage the risk to learn from minor risk.

Classification and Measurement - Risk of Harm

It categorizes the type of online risk of children, further identifying that risks vary depending on how they interact with the digital environment.

- Concerning detrimental values and commercial/persuasive risks problems, sexual harms to children, violence, and aggression of various forms, the online risks are the occasion's concern.
- Secondly, online risk harm is emphasized on the child's role in internet use.

2.7. Prevalence of Child Abuse and Its Impact

This section elaborates on the study made on the prevalence of child abuse and its impacts. Concerning the various research study child abuse, it can be observed that child abuse is an increasing problem with children across the world based on the various clutters, classes, education background, income level, and ethnicity. In few contraries, child abuse and exploitation were accepted socially according to the commitments of human rights and requirement of child development (General Assembly, 2006). With an increase in education and global socio-behavioral transition, the perception of child abuse has changed, and different countries have made different policies to suppress such online cyber-exploitation cases.

The right of child protection from exploitation, abuse, and violence is not a choice but rather a compulsion based on international law (UNICEF, 2005). Noticeably, most of the research has been emphasized to prevent the child from violence and abuse (Landers, 2013). However, some research also stated that it explores online offender behavior and children's experience of online abuse (Beech, 2014; Bifulco, 2014; Davidson et al., 2016). Research conducted by Davidson et al. (2016) in four Research targeting 4 EU countries that included national police and retrospective children and young people's exploitation surveys identified that most young people, about seventy

percent never received requests for sexual behavior online during their formative years, and seventy-nine percent were never asked to meet to engage in sexual activities(Davidson et al., 2016)

Thus, considering the above-stated vital aspects of online child abuse, it becomes inevitable to derive or conceptualize specific practical preventive measures. This research work or thesis intends to conceptualize a robust internet safety model to avoid online child abuse cases. It can be stated as a driving force behind this study. In this relation, the following sub-sections brief some of the critical pieces of literature pertaining to the children and internet safety systems.

2.8. Children and Internet Safety

This section discusses a snippet of the different approaches suggested for online child abuse prevention or safety.

2.8.1 Internet Stockholders Approach (Integrated Approach)

The discussion of the internet stockholders' approaches has been given in this section. The significance of an integrated approach to sexual exploitation from end-to-end multi-agency working is recognized (Pearce, 2014; Jago et al., 2011; Cockbain et al., 2014). Early detection from Serious Case Reviews emphasizes coordinated response fails (Myers and Carmi, 2016; Side Botham et al., 2016). Supporting disrupting perpetrators and sexually exploited children are intricate processes that need suitable and effective interventions from a set of identified stakeholders. Multi-agency methods allow organizations to provide their exact role while also raising shared actions to defend young people and proactively investigate abusers (Berelowitz et al., 2014). Safeguarding arrangements can be organized through Multi-Agency Sexual Exploitation (MASE) meetings and initiatives by a Multi-Agency Safeguarding Hub (MASH). Multi-agency arrangements may include sexual exploitation having issues like drugs and alcohol, violence against women and girls, gang association, trafficking, and missing (Home Office, 2014; Marshall, 2014; Barnardo's, 2012). Whatever the exact set-up of the inter-agency arrangement or multi-agency, the critical factor is the regulation of classification of diver settlement (Harris et al., 2015; Larsson, 2014). Therefore, the structure should be selected where young people can feel at ease and not be subject to stigma or scrutiny (Drew, 2016; Gilligan, 2016). When accompanied by a

multi-agency commitment to shared outcomes at the strategic level (Lebloch and King, 2006), advantages of close working arrangements include the following:

- Sharing resources
- Encouraging information sharing to safeguard young people
- Establishing shared expectations and approaches
- Flexible approaches
- Expertise sharing

2.8.2 Government Approach

Internet governance is a multi-layered process and requires professionals from various fields to work together on different levels (Hubbardand Bygrave, 2009). Based on the broader perspective, division of Internet governance including the following six task areas(DeNardis and Raymond 2013):

- The policy role of information intermediaries
- Architecture-based intellectual property rights enforcement,
- Cyber-security governance,
- Access and interconnection coordination,
- Setting Internet standards, and
- Governing "critical Internet resources."

2.8.3 Multi-Stakeholder Approach

Cooperation and involvement of different actors are stated as a multi-stakeholder approach with a democratic basis. Similar to the context of environmental governance and sustainable development (Bäckstrand, 2006), it came along in the preaching around Internet governance as early as the 2000s (Kleinwächter, 2007). Internet infrastructure and governance are always altering. Internet society emphasizes formulating a better democratic basis and model for a multi-stakeholder process (Power, Morison, 2014). A limited number of researchers foresee that the multi-stakeholder model does not fit all the elements of Internet governance. They demand that the private sector perform some tasks while some should rely on the traditional state governance. Internet governance includes tasks that variegate from technical architecture to policymaking (DeNardis, Raymond 2013). Some researchers question the approach of Internet governance being a democratic process (Hill, 2014).

2.8.4 Educational Approach

An elaborate discussion of the educational approaches has been given in the current section.

A Safe and Secure Learning Environment

A prevention curriculum shall be joined with a safe and secure school environment for promoting confident and reverential relationships between peers between the academic community and includes broad scope in parent/carer engagement (Beckett et al. 2013). Social media facilitates the spread of wrongful gossip or images among peer groups. Some students are introducing other young people to exploiters (Gohir, 2013; Casey, 2015). Grooming and sexual exploitation occur during school days (Gilligan, 2016; Factor and Pitts, 2015). Sexual exploitation can involve peers in complex ways (Beckett et al., 2013). The school environment can act as a positive space for young people.(Berelowitz et al., 2015; Firmin, 2013). The curriculum, school policies, and school ethos all add to surroundings that enable exploitive practices and the attitudes that excuse them (Chakravorty, 2016). Creating an educational environment in which a "whole-school" approach to addressing is crucial in responding to violence and abuse, including CSE (Womankind, 2010; Coy et al., 2013). Efforts to prevent Child Exploitation (CSE) challenge attitudes and helps students to develop emotional and social skills (End Violence Against Women Coalition, 2011; PSHE Association, 2016). Specialist in-service training for teachers may be crucial. (McNeish and Scott 2015).

Educational Initiatives for Children

Support from schools and support from parents and friends assisted with the recovery of online grooming and sexual abuse(Whittle et al., 2014). E-safety guidance from schools is helpful for children from under-resourced households where parents lack confidence in using online media (Livingstone et al., 2015). Schools are a vital collaborator in guaranteeing online child safety (DfE, 2014; Shipton, 2011). Smartphones and tablets present their unique risk environments. Network-level filters are not applied to applications used on such devices. Three controls specific to app management use parental control applications(Ofcom, 2016), changing the settings to prevent in-app purchases, changing the settings to stop apps from being downloaded.

2.8.5 Parental Monitoring

Parents shall play a major role by learning to become experts at parental control tools on mobile phones due to the speedy uptake of mobile phones among children(Croll, 2016).

Current Policies and Technical Rules

This section discusses the current policies and technical rules taken by the parents to avoid child exploitation has been discussed.

Online Awareness

Parents must be made aware of internet security as children are becoming a vulnerable target on digital platforms. Parents shall be competent to educate children at home about the online risks and take defensive methods on online safety at home. It is to help minimize the likelihood of children being exposed to different dangers come across online.

Dealing with the Expected Risks

Recommendations are given to adults for ensuing the necessary steps that must be taken in order to limit the chances of an attacker pointing to systems and devices at home. It is as followed:

- Avoid public networks.
- Protecting data through privacy settings on social networks,
- Avoiding mistrustful e-mails or attachments
- Protect PC with a firewall to prevent attackers or malicious software from gaining access through the internet
- Ensuring anti-virus software is installed and maintained.

2.8.6 Social Networking Approach

E-safety comprises the protection of children using technology legally(Katz, 2016). It ensures that children and school staff are instructed on the principles of realizing and managing risks online. The literature suggests that the guidelines and strategies combined in the attempts of parents and school staff will provide a clear understanding of digital skills on e-safety(Schemer et al., 2014). Parents must keep in mind the implications of having thousands of child-friendly apps offered for children online. It

must be made mindful of the mensuration to assure that security and privacy are not exposed.

2.9. State of the art review of International Efforts

The growth of the Internet and online social networks has paved the way for numerous security risks, including privacy risks (Boshmaf et al., 2011; Mislove et al., 2010), sexual harassment (Wolak et al., 2008), identify theft (Bilge et al., 2009), malware (Baltazar, 2009), fake profiles referred to as Social bots (Boshmaf et al., 2011; Elishar, 2012) and many more. Online social networks allow users for exposing private details, including the status of a relationship, sex, birth date, name of the school, email address, contact numbers, and physical location, which in turn can be used in the virtual world as well as real-world for harming children (Boshmaf et al., 2011). In sync with the Indian scenario, different works of literature have stated that the children are experiencing various threats specifically targeting them. In the present era, children face threats concerning personal information safety related to Internet pedophiles or online predators. Risks and harms are mapped to various online activities, including harm from content, harm from contact, and harm from conduct (Hasebrink et al., 2012, Wolak et al., 2008). The second type of threat targeting children is related to risky online behaviors, including online communications with an unknown person, chat rooms for communicating with strangers, explicit sexual talk, and sharing photos and videos with unknown people (Wolak et al., 2008). The third type of threat targeting children is identified as Cyber-bullying, where bullying takes place with the use of various communication platforms, including email, chats, online social media, and mobile conversations where attackers may harass the victims by sending hurting messages, sexual remarks, publishing images and videos which may be embarrassing and engage in any other inappropriate activity (CRC, 2016; Mishna et al. 2009).

The online world has grown unprecedentedly and brought significant problems for law enforcement across the world, including anonymity and dispersion (Hinduja et al., 2008; Goodman et al., 2002). It has become practically impossible to identify the physical location of the perpetrator of the crimes executed through the Internet (Nationale 2011). Smooth information sharing is an essential part of the Internet. With high-speed network availability and improved ease of use, and broad reach, millions of

bytes of information or content are made possible quickly. Actors involved in the Internet act as an intermediary and carry out different activities, including content uploading, hosting content, storing content, archiving content, cataloging content, and providing physical access to content as in Cyber Cafes (MacKinnon, R, 2015; Freedom House, 2009). Internet is controlled directly or indirectly by intermediaries making governments and law enforcement agencies and putting a gap in regulating Internet and cyber-crimes (Cameron, 2015).

Internet is more and more getting a part of life, especially for children and youth, and the potential is identified and exploited for communication, including social networking, entertainment including online gaming, and academic activities, including information gathering (UNICEF, 2012). Internet is a constant and familiar presence through computing devices, mobile, and other communication technologies (Michael Chan 2015). The gap between offline and online is getting reduced day by day, and segregation is becoming meaningless. Global reach and anonymous nature are upbringing illegal activities growing exponentially, targeting children (Stanley 2011). Online pedophile networks are thriving, and sexual offenders are effectively exploiting the Internet for child exploitation. Convicts are widely using the Internet for disseminating pornographic images, videos, and textual stories in the form of blogs (Bryce G. Westlake et al., 2011).

Protecting Children Online is identified as a challenge globally, and an approach spanning the globe is required for the same. Research efforts are already underway, with more reach at the Global level than at the national level. International Telecommunication Union (ITU) has established the Child Online Protection-COP (ITU 2015) strategy for creating an international network collaborative in nature for promoting online safety of children across the globe, in the year 2008 as a multi-stakeholder attempt within the Global Cybersecurity Agenda -GCA framework (ITU 2009). COP has taken an approach that emphasizes the functional relations between parts and whole for promoting child online safety and developing strategies in Law, Technology and Procedure, Organizational Structures, Capacity Building, and International Cooperation. COP brings together and forms partnerships from all social groups of the global community to ensure a safe and secure online participation for children everywhere, including international organizations, Commonwealth

Cybercrime Initiative-CCI, Commonwealth Telecommunications Organization-CTO, European Commission's Safer Internet Programme, European Network, and Information Security Agency ENISA, Insafe, International Criminal Police Organization-Interpol, United Nations Children's Fund-UNICEF, United Nations Office on Drugs and Crime-UNODC, United Nations Interregional Crime and Justice Research Institute-UNICRI and United Nations Institute for Disarmament Research-UNIDIR and many private organizations.

Harvard University's Berkman Center has started a research project for Internet and Society relating to the online safety risks faced by children in developing countries and is focusing on child and parent Internet behaviors. The Internet Safety Technical Task Force -ISTTF was formed in the year 2008. It was formed as a group of Internet businesses, non-profit organizations, academics, and technology companies to identify intended tools and technologies for creating an environment where youth can safely use the Internet (ISTTF 2008). As per the announcement by the Attorneys General Multi-State Working Group on Social Networking and MySpace in January 2008, a task force was created in concurrence of opinion with the "Joint Statement on Key Principles of Social Networking Safety."

The US has enacted the Children's Online Privacy Protection Act of 1998 -COPPA effective from 1st April 2000, applying to the collection of personal information by persons or entities under U.S jurisdiction for the children under 13 years of age by online activities (FTC 2016). COPPA is enforced by the Federal Trade Commission-FTC, which is authorized to issue regulations. COPPA is designed as a federal law aiming to limit the Internet service providers and websites from collecting and using information which personal about the children. The act was enacted after a survey conducted by FTC in 1998 on 212 websites that found personal information is collected by 89 percent of the websites, and 46 percent of them are not disclosing the fact and not explaining how the information is used.

ECPAT International has been formed as a network of organizations and individuals globally, working together with 90 members from 82 countries, including large coalitions of NGOs and small grassroots organizations to eliminate child prostitution, child pornography, and the trafficking of children for sexual intentions (ECPAT 2016). Connect Safely is a non-profit organization founded in 2005 is training users of

connected technology about various issues related to safety, privacy, and security and focusing on periodic safety tips, a guidebook for parents as well as caretakers, recommendations, news, and illustrations on aspects to the effective use of technology and implementation of policy (ConnectSafely 2016). The second Tuesday of every February is celebrated as Safer Internet Day as an awareness-raising effort spanning over 100 countries by ConnectSafely. The European Commission launched Safer Internet Programs in 1999, renamed as Better Internet for Kids-BIK in 2012 following the adoption of European Strategy to "Make Internet a Better place for Children" to support projects and events to promote self-regulation among industry and international cooperation (BIK 2016). Safer Internet Centers are made up of knowledge centers and helplines in a pan-European network called INSAFE (BIK, 2016) and hotlines organized in a unique pan-European network called INHOPE members, Iceland, Russia, and Norway (INHOPE, 2016).

Federal Bureau of Investigation (FBI) has released a parent's guide to safety for protecting children from the online and offline world, and a Cyber Tip Line system was introduced, which was made operational by National Center for Missing and Exploited Children in partnership with the FBI and other law enforcement agencies (NCMEC 2016). In addition to this, a national sex offender registry is maintained for protecting kids in Cyberspace.

SaferNet, a Brazilian non-governmental organization formed to combat crimes related to the Internet in partnership with the Federal Public Ministry, facilitates anonymous reporting and provides information and training about Internet safety and security (Safernet 2016). Additionally, SaferNet helps in anonymously facilitating reporting of crime, prevents and investigates the reporting of crimes targeting child including pornography, identity theft, and various other crimes, including hate communication. SaferNet has taken the responsibility of education and training, mobilized the public on issues related to their rights and safety, and worked with the government to improve legislation for crimes related to the Internet.

Childnet International UK is a non-profit organization targeting to make the Internet an excellent and danger-free place for Children (Childnet, 2016). They provide tips, games, and Internet safety information to help the young people, safety resources to teachers and professionals to safeguard the workplace and young people associated with

them, and advice for parents and caretakers for supporting children and youngsters for safe and worthy use of the Internet.

Internet Watch Foundation UK acts as a hotline for reporting criminal online content, including abuse content that is sexually hosted anywhere globally, age-inappropriate content hosted in the UK, and graphical child sexual abuse images hosted in the UK (IWF, 2016). Around 130 companies worldwide support IWF for fighting against content that is sexual abuse in nature.

Safespace Qatar helps parents and teachers keep children safe online; the MOTC (formerly known as the Ministry of Information and Communications Technology) launched SafeSpace.qa, a website with worthful information on cyber safety (Safespace 2016). Safespace provides awareness towards content management in social networking sites, safety practices, and guidance in using all technological applications available on mobile and computers.

Virtual Global Taskforce was established in 2003 for building an effective, partnering international law enforcement agencies, Non-Governmental Organizations, and industries for helping and protecting children from online abuse and various other forms of multinational child sexual exploitation (VGTF, 2016). Various law enforcement agencies from 13 different countries are part of the initiative.

Australian Communications and Media Agency is administering a complaint mechanism for Australian residents and law enforcement agencies for reporting online content forbidden by law, including child sexual abuse material (ACMA 2016). Alanahh and Madeline Foundation Australia was founded in 1997 with a central goal for taking care of children who have undergone severe violence, reducing the incidence of bullying, cyberbullying, and similar cyber risks, and counsel for the safety and welfare of children (AMF 2016). The National Centre Against Bullying -NCAB, an initiative of the Alannah & Madeline Foundation, which is an apex body working on appraising and communicating the Australian community on the issue of childhood bullying and the creation of safe schools and communities, including the issue of cyber safety(NCAB 2016). Netsafe New Zealand is an independent non-profit organization for enabling online technologies in a secure and safe mode. In conjunction with other national and transnational organizations, strengthening and extending online safety

awareness and education and extending support services are required within the country (Netsafe NZ, 2016).

Table 2.1: Children Online Safety International Efforts

International Body	Purpose	Constituents	Outcome	Remarks
(International Telecommunication Union, 2015)	To promote online safety to children across the globe	Commonwealth cybercrime initiative (CCI), the European commission's safer Internet program, European network and information security agency (ENISA), Insafe, international criminal police organization (Interpol)	Child online protection (COP)	In entirety, all international bodies are intended to serve for online safety of children irrespective of their initiation
(Internet safety technical task force, 2008)	To Create risk-free environment over the Internet	Internet businesses, non-profit organizations, academics, and technology companies	Tools and technologies for the purpose	
(MySpace technology company, 2008)	To prevent access by the children under 14 years	MySpace and Attorneys General	Technologies and regulations	
(Federal Trade Commission USA, 2002)	To avoid the collection of personal information of children less than 13 years old	---	Children's online privacy protection act (COPPA)	
(End child prostitution and trafficking International, 2018)	To eliminate children prostitution and trafficking	Global civil society organizations like NGOs	Reduced trafficking	
European commission's Safer Internet Programs (BIK Team, 2019)	To provide better Internet for children	knowledge centers, help lines, and hotlines	Improved Internet safety	
(National Center for Missing and Exploited Children, 1998)	To protect children from online risks	FBI and National center for missing and exploited children (NCMEC)	Safety guide and cyber tip line system	

(SaferNet, 2018)	To provide information and training about Internet safety and security	Federal public ministry, the Brazilian government	Reduction in children targeted crimes
(Childnet international UK, 2018)	To make the Internet a risk free platform for Children	---	Safety resources and guidance
(Internet Watch Foundation, 2013)	To fight against sexually abusive content	Around 130 companies	Portal to report online criminal incidents
Safespace Qatar (Ally et al., 2016)	To keep children safe online	---	Safety measures and guidance technology use
(Virtual Global Task Force, 2017)	To protect children from online abuse	Law agencies, non-governmental organizations, and industries	Collective system to fight online risks
(Alanahh and Madeline Foundation, 1997)	To reduce violence, bullying, and counseling for safety	The national center against bullying (NCAB)	Reduced violence
(Netsafe New Zealand, 2018)	To enable safer online technologies	National and transnational organizations	Safer online tools
(EU Kids Online, 2014)	To enhance European kids online knowledge	---	Increased online knowledge of kids
(Aarambh India, 2014)	To prevent child sexual abuse	Prerana NGO and ADM capital foundation	Online resource portal and Internet hotline to report abusing content

EU Kids Online is a transnational research network seeking to raise the knowledge of European children's online chances, sources of danger, and safety (EUKids, 2016). Multiple methods map the Internet's user experience, especially parents and children, by talking with various stakeholders at the national and European levels. The program is funded by the EC's" Better Internet for Kids program."

Microsoft has shown its commitment to online child safety. As a step towards awareness, it started providing exclusive tips on the subject and has introduced a Family safety filter and parental controls in its various versions of operating systems

(Microsoft, 2016). Google has introduced the child-friendly search engine Safe Search kids, enabling filtered search (Google,2016). Google also provides parental control features to block, restrict, limit, or access different features for younger children. The summarization of major international efforts towards children's online safety is made in Table 2.1.

The benefits of ICT to users are with the cost of inappropriate content. As online safety is a global issue, many countries initiated actions to attain it. Sexual offenders effectively use the Internet to exploit children by disseminating pornographic images, videos, and textual stories as blogs. Parental control software tools are essential to reduce online risks for children. Inappropriate content such as child abuse material can be blocked at the ISP level with the help of police and child care organizations.

The online risks may be content, information security risks, and behavioral risks. Cyberbullying is a common threat to children on the Internet. A review of international efforts towards children's online safety shows that many organizations are trying to end online threats to children. The international bodies assist children online with different tools, technologies, regulations, protection acts, safety resources, education, training, guidance, safety measures, crime reporting system, and children-friendly search engines.

2.10. Conclusion

In this chapter, primarily, the critical pieces of literature on the online risks for children and policies issues and available solutions for Online Child Exploitation and Internet Filtering Techniques and policies to protect them as Internet users were discussed. The predominant objective of this chapter was to assess different kinds of literature presenting offsets estimation in Child Exploitation for Online Risk and allied solutions to ensure Issues pertinent to online child safety and protection. The next chapter discusses the research design and conceptual research model, and methodologies used in the research. It examines direct and indirect policy measures available to help mitigate risks for children online, present and compare existing and planned policy approaches for the protection of children online and explore how international cooperation can enhance the protection of minors on the Internet.

CHAPTER 3

R E S E A R C H D E S I G N

3.1. Introduction

Stating the previous efforts in this study, the introduction of the presented study was well discussed in the first chapter that provided the theoretical foundation for the current study. All key factors about child online safety were discussed in previous chapters. It enabled the researcher to place the findings within a proper context to render them more meaningful. After that, the literature review throws up the precise research matter and allied question that this study attempts to address. The chapter predominantly discusses the research design and the snippet of fundamental methodological paradigms based on the research questions and objectives. This study can be stated as a behavioral assessment paradigm where the respective perception of the allied stakeholders has been assessed to identify critical factors that impact the techniques and decisions to prevent online child exploitation. The overall research intends to assess different causative factors of online child exploitation, risk mitigation, and preventive approaches to avoid online child exploitation. To meet the objectives of the study, both primary and secondary data have been collected. Semi-structured questionnaires have been constructed and administered.

Realizing the significance of the different stakeholders such as children, parents, tech-experts and legal experts who can help to identify different psychological traits signifying online harassment symptoms, behavioral changes, online surfing behavior, causes of exploitation, need and optimal model of inline internet usage and different preventive measures to avoid child (online) exploitation, this study employs both qualitative as well as a quantitative method. Qualitative methods helped explore secondary data sources to understand contemporary child online exploitation scenarios, different reasons, cases of child online harassment or exploitations, abuses. Also, secondary data-based qualitative assessment enables identifying different approaches or techniques available to perform web-content filtering or monitoring to avoid any possible child exploitation. At hand, complexities, issues, and future scopes are identified using the qualitative method. In the quantitative method, different stakeholders, including children, parents, technical and legal experts, have been interviewed to assess their respective perceptions towards internet surfing, online crimes, harassment cases, causative factors, and remedial measures. This research can

be stated as a mixed research paradigm with analytical and empirical approaches for conducting at hand study.

3.2. Research Background and Justification for Indian Context

The online world has grown unprecedentedly and brought major problems for law enforcement worldwide, including anonymity and dispersion (Hinduja S et al.,2008; Goodman et al., 2002). It has become practically impossible to identify the physical location of the perpetrator of the crimes executed through the Internet. Smooth information sharing is an essential part of the Internet. With high-speed network availability and improved ease of use, and broad reach, millions of bytes of information or content are made possible quickly—actors involved in the Internet act as an intermediary. Intermediaries carry out different activities, including content uploading, hosting content, storing content, archiving content, cataloging content, and providing physical access to content as in Cyber Cafes(MacKinnon, R 2015, Freedom House 2009). Internet is controlled directly or indirectly by intermediaries making governments and law enforcement agencies and putting a gap in regulating Internet and cyber-crimes (Cameron 2015).

Internet is more and more getting a part of life, especially for children and youth. The potential is identified and exploited for communication, including social networking, entertainment, online gaming, and academic activities, including information gathering(UNICEF 2012). Internet is a constant and familiar presence through computing devices, mobile, and other communication technologies(Michael Chan et al.,2015). The gap between offline and online is getting reduced day by day, and segregation is becoming meaningless. Global reach and anonymous nature are upbringing illegal activities growing exponentially, targeting children(Stanley, 2001). Online pedophile networks are thriving, and sexual offenders are effectively exploiting the Internet for child exploitation. Convicts are widely using the Internet for disseminating pornographic images, videos, and textual stories in the form of blogs(Bryce G. Westlake et al., 2011). Additionally, pedophiles use social networking sites, newsgroups, and chat rooms to deceive themselves as children for sexual communication(Wolak et al., 2008).

Online child safety is a global issue. It requires a global response. Many countries have taken steps to battle with it by introducing online child safety-related acts and initiated

various awareness programs (Livingstone et al., 2014; Isaac et al.,2014; ITU, 2015; UNICEF,2012). The preparation of standards and guidelines for children or young people, parents, caretakers, pedagogues, policymakers, and industry is taken up by few international research organizations (O'Connell, 2003; ITU, 2015).

When it comes to the growing Internet users, especially children, India is not much behind other developed nations(IAMAI, 2015). Hence, foreseeing the need for online child safety, the Govt. of India has taken the initiative towards formulating a separate sub-section (section 67 B) on online child safety in its Indian IT Act 2000 and Indian IT Act Amendment 2008 (IAMAI 2015; Indian IT Act 2000; Indian IT Act Amendment 2008).

In 2017, the National Commission for Protection of Child Rights (NCPCR) launched the POCSO e-box, enabling children who are victims of cybercrimes to lodge complaints. The scope of the POCSO e-box is enhanced so that cases belonging to cyberstalking, cyberbullying, morphing, and child pornography can be reported. Victims, friends, parents, guardians, and relatives can report cybercrimes through the e-box facility at the website www.npcr.gov.in. Reporting or complaints can also be made through mobile numbers and email. E-box is identified as a direct channel for reporting under the Protection of Children from Sexual Offences Act, 2012. There is no centralized mechanism in India for the dynamic monitoring of Online child sexual abuse materials (CSAM). The inter-ministerial committee constituted by the Ministry of Electronics and Information Technology(MeitY, 2017) deliberated and brought out the issues related to CSAM and methodologies for blocking in India. Depending on the committee Ministry of Electronics and Information Technology recommendation, MeitY has issued an order to Internet Service Providers(ISPs) to adopt and implement Internet Watch Foundation(IWF) resources for preventing online CSAM in India. There is much more left to be done in India to ensure the full safety of teenagers.

3.3. Research Question

This research question is:

Research Question 1: How to improve child online safety in the Indian Context?

3.4. Research Objectives

In the last few years, escalation in the exploitation of the internet by the people of different age groups has forced the allied authorities and industries to restrict some websites or some user-specific content to confine the cyber-crime. It is noteworthy that there are now specially developed numerous techniques to prevent the exploitation of children who visit online websites and provide their details while logging on to any website. Hence, the principal goal of this research or study is to assess (empirically) internet security techniques to safeguard the users and their data from being misused. Undeniably, the internet has become an inseparable part of people of almost all ages, each having its region of interest. While some access online sites and data for knowledge the others access it for entertainment. Noticeably, children nowadays also access online content for educational purposes, and it cannot be denied that the internet brings lots of opportunities to children. However, it is also noteworthy that children's exploitation of the internet exposes them to new risks and dangers. Hence, this research aims to prevent children from risks encountered while accessing online content since online child exploitation has been a concern across the globe. Noticeably, children are more prone to face the risks associated with cybercrime and finally end up harming themselves or the people associated with them. In this research, several constructs associated with facilitating safe online content access for children have been examined. The research has ensured that the study discusses and provides information about aspects allied with the mitigation of cyber-crime, focusing on protecting children from the harm caused due to cyber-crime.

The principal goal of this research is to assess the perception of the different stakeholders, including children, teachers, parents, technical and legal experts, to understand root causes, behavioral perception, and possible solutions to avoid online cybercrime and (online) child exploitation. The research also intends to assess the efficacy of the different web-content filtering, risk-mitigation measures, and parental control paradigm to prevent online child exploitation cases in India. With these motives, the following research objectives have been identified.

- To examine the distinctive issues pertinent to online child safety and protection

- To analyze the adult content identification mechanisms based on E-discovery techniques
- To study and examine the existing global practices addressing Child online safety
- To study and examine the risk mitigation framework addressing children online issues in the Indian Context.

3.5. Research Design

Increased growth of ICTs, high-speed connectivity, and wider network coverage made online activities more manageable and often harmful across the globe. To protect children's rights, Internet governance practices have to be strong in this digital era. The Internet governance organizations can incorporate multiple stakeholders such as children, parents, teachers, Internet service providers, law enforcement agencies, and governments for their better performance.

As children's online safety is a global issue, several countries have taken steps to act on it by introducing online child safety and protection-related acts and various awareness programs(Livingstone and Smith, 2014; Isaac et al., 2004; ITU, 2015; UNICEF, 2012). In this regard, the guidelines are prepared for children, parents, caretakers, policymakers, and industry by international research organizations (O'Connell 2003; ITU, 2015). The children's online safety issues may be addressed within the categories such as governance, technology, and society.

3.6. Addressing Issues: Governance, Technology and Society

High-speed growth in the functionality of Information and Communication Technologies coupled with high-speed connectivity, more comprehensive ranges of services, on-the-fly entries, and exits of mobile has made accessible provision for online activities for users across the globe, including children. It is being an essential part of society and acting as a centralized platform for facilitating social activities. In parallel, the new technologies are setting the stage for various types of crimes targeting people across all age groups online and offline based on user practices. It is essential that Internet governance practices have to make strong consideration for children's rights in the digital era. With the rapid growth of the Internet in India and other developing nations, Internet governance organizations shall shape best practices, including multiple

stakeholders, children, parents, teachers, Internet service providers, law enforcement agencies, and governments.

Dependent variable Child Online Safety

Child Online safety is a global issue and requires a global response; many countries have taken steps to battle with it by introducing online child safety or protection-related acts and initiated various awareness programs(Livingstone et al. 2014; Isaac et al.,2014; ITU, 2015; UNICEF, 2012). The preparation of guidelines targeting children, parents, caretakers, pedagogues, policymakers, and industry is taken up by few international research organizations(O'Connell, 2003; ITU 2015).

3.7. Explanatory Variables-Governance

3.7.1 Security Awareness

Awareness programs (NIST, 1998) are identified as the mode of public awareness of the negative consequence of Internet use, an uninterrupted undertaking aimed at building and holding a security-positive environment. Sources of safety awareness include traditional media, websites, specialized awareness materials from experts, Internet service provider level. Attention to new policy focus is urgently needed for awareness-raising and backing measures projected for suiting the needs of young Internet users(Livingstone. et al., 2012).

3.7.2 Proliferation and Controlling

The proliferation of the Internet has significantly contributed to the increase of pornographic or sexual material availability and changed the way children can consume sexually explicit materials(Owens et al., 2010). It has enhanced the probability of children accidentally accessing such content on the web. Technical measures are essential for assuring the children of the possible risks and associated threats they face online. Regulatory responsibilities for online risks and opportunities shall be distributed among various stakeholders, including government, industry, academia, law enforcement agencies, child welfare services, parents, and children themselves. (Livingstone et al.,2006).

3.7.3 Practices and Guidelines

National policies for protecting children online are complex, wherein policies are trying to accept different risks and initiatives from several stakeholders existing at different

levels as a challenge (OECD 2012). Identified risks for which children and youngsters have been exposed without a shield increase the need for different policy issues. Practices and Guidelines are formulated by incorporating child rights consideration into suitable policies and processes at the corporate level, developing standard processes for handling child abuse material, and creating a safer online environment for all age groups. Policies and guidelines are focused on educating children, teachers, and parents about the safety of children online and the worthy use of ICT and promotion of digital technology to increase civic engagement(Adler et al.,2005; UNICEF 2014).

3.7.4 Grievance Redress

A well-defined governance mechanism for an online grievance redress system (Rana et al., 2013) involving a system of online registration, investigation, and response within a time frame is identified. Grievance redressing mechanism commonly used in India as management and governance-related process shall be extended for handling children's online threats.

3.7.5 National Framework

The national framework shall be introducing a novel way of defining the workforce with responsibility for keeping children safe and establishing a set of competencies and standards for people having direct or indirect contact with children to ensure that they are delivering a systematic and consistent standard of help and aid to children and young people (Hasebrink 2008).

3.7.6 Certification Initiatives

Widely accepted preventive measures, awareness, and education by civil societies, industry, government initiatives, and motivated individuals focus on online etiquette for children. Existing awareness programs designed for children and young people are not system-wide(UNICEF 2016). Awareness programs for children in system-wide need to be implemented by adequately accommodating the high school and higher secondary curriculum. MEITY, the Ministry of Communications and Information Technology, has initiated a five-year project on "Information Security Education and Awareness" (ISEA 2021), which widely promotes information security awareness among children, home users, and non-IT professionals. Centre for Development of Advanced Computing executes the project(CDAC 2021).

3.8. Explanatory Variables - Technology

3.8.1 Self-Efficacy

Social networking sites enable users to share minute updates to friends, including the status feeling, cognition content, and any specific behavior or action (Jones et al. 2008, Valenzuela et al., 2009). Self-disclosure of personal information and status updates may become problematic because of the identified risks, including identity theft, cyber-stalking, and cyberbullying. In contrast, users are more concerned about privacy, while self-disclosure is widely spread (Jones et al., 2008).

3.8.2 Safety measures

- Type of passwords(weak or strong)

Passwords play a vital role in web user's experience(Florêncio, D et al., 2007). Strong passwords will not protect users from password-stealing attacks, including crucial logging and phishing attempts but help from brute-force attacks, guessing attacks, and shoulder surfing(Florêncio, D et al., 2007).

- Knowledge on safety issues for chatting with unknown people

Predators provoke young people to participate in offline sexual activities and broach the process by discussing sexual nature by sending pornographic materials facilitated by children's interest using chat rooms(Normand, C. L et al., 2016). Websites or applications with chatting blogs have been identified as sites with greater prevalence (YISS 2011).

3.8.3 Application trust

Privacy is considered the dominant concern for developing new applications for interactive technology(Palen L et al., 2003). Frequency and usage type of social networking sites coupled with Internet skills are correlated with modifications in privacy settings (Hargittai E. 2010). Privacy management includes continuous management of boundaries between different actions like disclosure, identity and temporality, and rule-setting and enforcement (Palen L et al., 2003).

3.8.4 Virtual Harm Exposure

- Identification of virtual harm

Victimization through Internet, termed as Cyberbullying, is defined as "willful and repeated harm inflicted through the medium of electronic text "(Patchin, J. W et al., 2006). Cyberbullying is an encapsulation of all forms of harm or harassment that commonly occur with the Internet, computers, and mobiles which includes sending threatening, harassing, and harmful mails or messages, posting derogative comments or intimidating anyone online, ignoring, disrespecting, spreading rumors, stalking or physical threatening (Hinduja S et al., 2007).

- Response action for age-inappropriate content

Video sharing sites are associated with age-inappropriate content, including violent and pornographic content(Livingstone et al., 2013). Though parents support their children's Internet usage, setting limits of use, including content types and time, is identified as a struggle. Several existing tools are available to help parents limit exposure to age-appropriate content(Hashish Y et al., 2014).

3.8.5 Frequency of use

- Amount of time spent on the Internet

Children are spending more time on the Internet and engaged in a variety of online activities. Various concerns are identified, including cyberbullying, easy access to age-inappropriate content, addiction to the Internet, and privacy issues(Livingstone S et al., 2011). It is hard for parents to monitor tech-savvy children and their use of the Internet and online activities and because Internet use has become more personal and portable (Shin W, 2015). Since the inception of the Internet, Internet addiction is identified as one of the most preoccupations (Burnay J et al., 2015).

- Reuse of same passwords

Password insecurity is a perception of security than reality(Ives et al., 2004). Several applications, including social networking sites, mobile apps, and other web applications, lead to a vast increase in the use of the number of passwords required. Creating unique passwords and changing them occasionally is important.

- Frequency of password change

Passwords have been identified as the crucial means for access control for various online activities (Florêncio D et al., 2007). The rapid increase in applications, including social networking sites, mobile apps, and other web applications, increases the number of passwords required. Changing the passwords occasionally is essential.

3.9. Explanatory Variables - Social

3.9.1 Cultural Characteristics

- Identification of strangers in the social networking profile and readiness to remove strangers from the friend list

Young Internet users should have the capability to identify Online Social Networking fake accounts, sexual content, and connection request from multiple accounts of the same person(Boshmaf et al., 2011). Awareness about children's activity while online is very much critical (Tsirtsis et al., 2016). Users are accepting the requests for connection sent by unknown, especially when a list of mutual friends have appeared in the strangers' friend list(Boshmaf et al., 2011)

- Sharing of passwords to friends and relatives

As a habitual behavior, passwords are shared with family members and friends (Zhang-Kennedy, L et .al 2016). One-third of the users share their passwords (Kaye 2011). As per surveys in the US, 30 percent of teens were ready to share their password with a friend, boyfriend, or girlfriend, an online practice that may compromise the safety online (Lenhart et al., 2011).

3.9.2 Individual characteristics

- Whom to be informed after bullying

The occurrence of cyberbullying can be identified as an intersection of tens, technology, and trouble (Hinduja et al., 2014). The primary challenge identified concerning cyberbullying is the lack of knowledge to consider this as harmful. Law enforcement worldwide is hesitant to take the issue due to a lack of clear evidence of a crime or physical safety issue(Hinduja et al., 2014). Parents, teachers, and law enforcement agencies shall be aware of the issue and know how to respond once informed.

3.9.3 Parental Mediation

- Children interaction with parents related to online activities

The role played by the parent in identifying how their children use media is crucial. Parental mediation exists for the use of television defined under the extensive and systematic plan of parental regulation and mediation, which is active, restrictive, and co-viewing in nature. An elaborate and systematic plan of mediation, if any, shall be practiced in determining the use of the Internet at home(Livingstone 2008). Parents

playing to gain the opportunities and understating the risks in Internet use is identified as one of the pressing questions regarding the psychological effects of media use(Appel 2014).

3.9.4 Openness and coping

- Information about technology and online activities parents and teachers should know

Parents and teachers do a great job supervising youth at school and home. Nevertheless, many adults lack the technological know-how to keep track of what their children are doing online. As a result, the victim's experiences may be missed, and predator actions may be left without a check(Hinduja et al., 2014). Parents and teachers shall educate online behavior and develop and promote teen guidelines (Holloway et al., 2013).

3.10. Conceptual Research Model and Research Hypothesis

The conceptual framework derived based on the guidance of theoretical and empirical background previously reviewed is shown in Figure 3.1. The conceptual framework drawn for this confluent mixed-method design involves multiple studies depicting the relationship between governance, technology, social factors, and children's online safety issues.

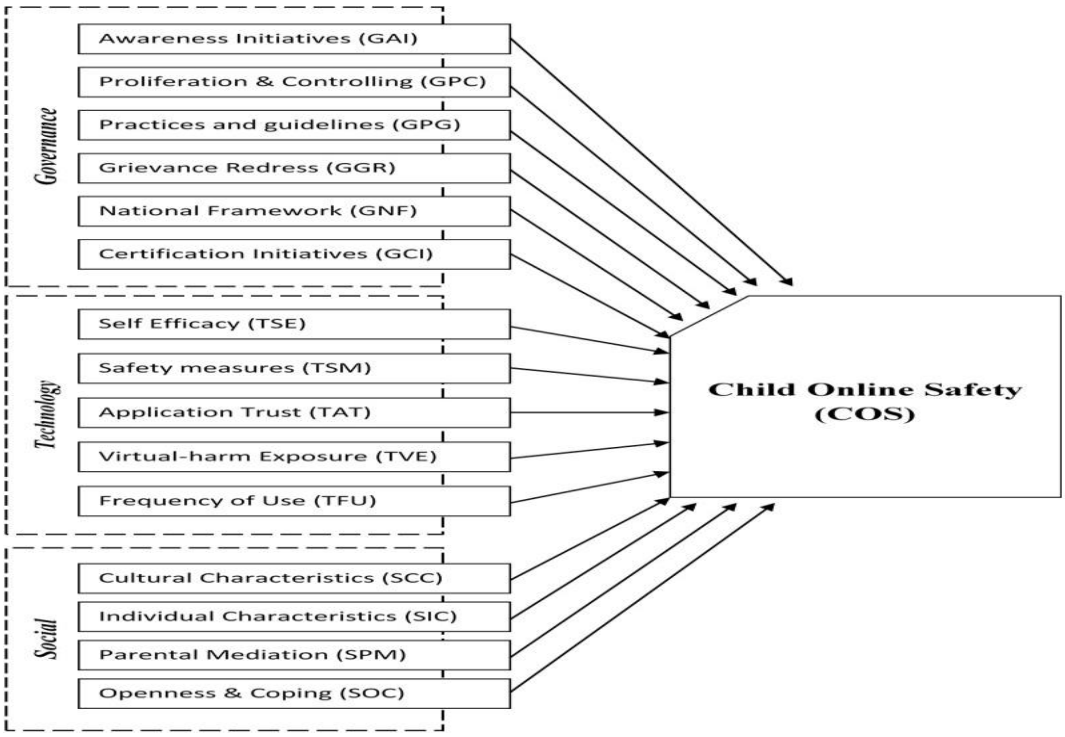

Figure 3.1: Conceptual Research Model

Considering the above-stated objectives and research intend, based on an exploratory assessment of the secondary sources, a few research hypotheses have been framed. Some of the key hypotheses identified for the at-hand research are given as follows:

H_{01}: Online activities do not have a significant impact on the socio-educational development of children.

H_{02}: Socio-behavioral monitoring on the internet cannot help avoiding online child exploitation.

H_{03}: Log-based parental control technique and auto-information exchange measures do not significantly impact cyber-crime avoidance.

H_{04}: Forming and implementing strict online content filtering and monitoring regulations cannot effectively alleviate online child exploitation.

H_{05}: Measures taken for reducing the impact of online child exploitation do not seem to be effective.

H_{06}: Developing inter/Intra socio-administrative platforms with online activity and content monitoring access cannot help avoiding online child exploitation.

3.11. Research Methodology

Research methodology signifies an orderly arrangement of approaches applied in research to collect factual information or data, which can be applied as a basis for grounding subjective or intended inferences and interpretations to explain the subject matter, research aims, and predict illations(Miles et al., 1994; Mouly, 1978). Conventionally, the word methodology signifies the approaches and paradigms allied with the positive approach for evoking responses from respondents based on pre-defined research questions, characterizing processes, and demonstrating experiments (Cohen & Manion, 1994). The methodology is employed to the approaches and paradigms applied by researchers. The methodological aspects of the study are appropriately referred to as the scientific philosophy incorporated both within the approaches and within the researcher's methods for data collection and respective investigation (Pole et al., 2002).

Kaplan defined Research methodology as the "paradigm to characterize and assess the research evolution, various involved practices and approaches, throwing glance on respective limitations and resources, justifying their presuppositions and eventual results, relating its capabilities to the twilight zone at the frontiers of

knowledge"(Kaplan, 2004). The research methodology comprises operating rules and principles guiding particular targeted scientific exploration and objective assessment(Robertson, 2000). Research methodology facilitates various important functional rules and guidelines to collect associated justifiable evidence about what occurs and why it occurs. It enables researchers to verify the generalized hypothesis and verify the findings. Research methodology is the well-defined and organized approach applied by a researcher to perform the study, analysis, and cross-verification towards particular predefined research objectives. Research methodology must be establishing a relation towards the formulation of research strategy and contributing to the well-defined, organized structure of a research objective. Research methodology can be regarded as the phenomenon of reaching specific dependable resolutions or solutions to issues through well-defined and planned data collection, data analysis, and data interpretation. Research methodology is crucial and the most effective tool for advancing knowledge, introducing and promoting progress, and relating more efficiently to its environment, accomplishing its objectives and exclusively associated conflicts.

The research methodology comprises the overall research and study paradigm incorporated and applied for the research objectives. An optimistic and well-defined methodological preparation is a significant requirement for quality research that helps researchers an optimistic, scientific and feasible approach for procedural implementation, problem-solving, and realization. Considering the need for the precise and crisp presentation of research methodology about the current study titled "Child Online Safety: A Select Study in Indian Context," this section predominantly discusses the snippet of fundamental methodological paradigms.

Stating the previous studies' previous efforts, the introduction of the presented study was well discussed in the previous chapters that provided the theoretical foundation for the current study. All key factors of child online safety were discussed in Chapter 1 and Chapter 2. Literature review threw up the precise research matter, and allied queries and questions attempted to address in the current study. The pilot study undertaken by the researcher accordingly indicated changes in the methodology required for this investigation, and the changed final methodology was posited. The activities enabled the researcher to place the findings properly to depict them in a more meaningful

manner. It, in turn, provided the theoretical framework for the investigation. This study can be stated as a behavioral assessment paradigm where the respective perception of the allied stakeholders has been assessed to identify critical factors that impact the techniques and decisions to prevent online child exploitation.

Additionally, various approaches to prevent children from viewing explicit content on the internet have been discussed. To achieve precise results, the demographic and descriptive constructs of the stakeholders have been accessed. Exploring these factors exploiting both available literature and first-hand data, also called primary (response) data, must. It motivates the author to employ mixed research paradigms, including qualitative and quantitative research methods. A snippet of the methodology under consideration is discussed in the subsequent sections.

Study analyses factors that help filter techniques and preventive measures against online child exploitation, such as creating awareness about online child exploitation, proper rules, and guidelines against cyberbullying. Most scholars implement different methods to carry out the research, which depends on the purpose of the research and the type of information required. Both qualitative and quantitative research methods are used (Porter and Coggin 1995). The qualitative method has been proposed because it can answer why, how, and in what way. Considering the various filtering techniques and preventive measures of online child exploitation, the empirical study encompasses semi-structured interviews with the different stakeholders to collect responses towards varied factors affecting the successful assessment of opportunities for the stakeholders. Meanwhile, the quantitative approach also has great significance in assessing various vital aspects of intended research work and is equally vital as qualitative research. Hence, this research intends to employ questionnaires and surveys to collect numerical or measurable data from targeted respondents. The researcher's expectations of getting a more comprehensive representation of what is expected are also part of the proposed quantitative research. As already stated, this study encompasses a mixed research paradigm that uses qualitative and quantitative research methods. The research collects primary data by preparing a questionnaire and conducting interviews with the different stakeholders of the research.

3.11.1 Research Paradigm

Qualitative Research Paradigm

Qualitative research is essential for achieving specific information, including conceptions related to behavior, values, perceptual experience, opinions or beliefs, and varied significant social contexts of specific, pointed populations. A qualitative research study comprises data collection and research questions lined up according to what is learned. Unlike quantitative research, qualitative research consists of the secondary sources-based investigation based upon looking up answers to questions, systematical use of a predefined set of procedures to answer the questions, gather evidence, produce findings. The qualitative research model explores the research objectives, key aspects, and variable analysis to formulate research hypotheses and critical constructs. The research would lay the foundation for keying or assessing various factors causing online child abuse, effective parental control techniques, log analysis to protect passwords, stakeholder's perception of rising online child exploitation, at-hand solutions, existing policies, and future scope.

In the qualitative research paradigm, data collection is carried out using integrated structured research instruments. The results provide reflecting behavior, perceptual experience, attitudes, and actions towards the desired goal. The qualitative research paradigm makes the overall research approach intensifier and flexile and enables the researcher to explore and assess. The results are usually based on smaller sample sizes and typically do not represent the population. It avoids the repeated performance or the replication of the research and promotes novel contributions towards future usage. Qualitative research often employs participant observation and in-depth interviews that enable the researcher to enter the world of the subjects, chiseled and integrated content that they find in reality, and then assess what they have gained from other materials. Qualitative research is a type of empirical research paradigm. Data is not needed to be in numbers but with extensive data on legion variables over an extended time frame (Gay and Airasian, 2000) to achieve key or powerful insights that cannot be retrieved through other approach paths. Qualitative research is not merely to duplicate what has been done already but also helps researchers explore existing works, extract information, and contribute to the world with better solutions and dynamic revelation

and propositions. The standardized exercise examines the maximum degree to which an outsider would support the research outcome with the data collected and processed. Qualitative research is essentially significant in obtaining specific information about particular populations' cultures, values, opinions, behaviors, and social conditions. Qualitative research design comprises data collection and research questions that are aligned according to what is acquired. Qualitative research comprises the secondary resources-based investigation based upon interviews, systematic use of a set of procedures designed beforehand to answer the questions, collecting proofs to make things evident, and bringing forth findings. The qualitative research model explores the natural backcloth of the research objectives, key prospects, and variable analysis to articulate research hypotheses and research constructs.

Quantitative Research Paradigm

Quantitative research is defined as the process of data gathering (especially the numerical data) to characterize, predict and control region of interest (ROI) or the process of interest(Gay and Airasian, 2000). Simply, quantitative research is defined as empirical research where the variables with considerable importance and the associated data are represented as numbers. Quantitative method is defined as *"*the process of assessing or investigating a social or human problem, based on certain defined and testing approach containing research variables, estimated with numbers, and assessed with statistical procedures, to estimate whether the predictive generalizations of the theory hold true or not*"*(Creswell (1994)). *Q*uantitative research primarily depends on numerical data and associated statistical evaluation and analysis. Quantitative analysis is the approach established upon certain statistical materials in association with the samples. It emphasizes analyzing a case variable matrix comprising survey data, which the researcher has either gathered through specific direct or indirect sources.

In summary, quantitative research data is collected through structured research instruments and eventually facilitates less information on individual character, personal attitudes, and allied reflecting motivation. Results used to be the reflection of the larger sample sizes. In general, quantitative research can be distinguished from the qualitative research paradigm due to the large numbers of samples in populations and the types of questions being asked.

Quantitative research mainly consists of numbers and statistics and encompasses methods that give enumerable outcomes. The counted brought together information to determine averages, highs, and lows, and an item's rankings compared numerically with another. The quantitative study intends to perform primary data-based research work. Based on a particular effective questionnaire, responses would be collected from the different stakeholders about online child exploitation. To assess different research constructs such as the personal attributes and perceptions towards online child abuse, perception towards internet use by children and its impact on their socio-behavioral aspects, online child exploitation, different existing policies, limitations of the existing online digital filtering systems, and possible approaches different stakeholders have been interviewed through the semi-structured interview process. Noticeably, to augment research generality and acceptability for the targeted research issues, the data is collected from primary data sources and the secondary data sources in this study. A snippet of the applied data collection techniques is given in this section.

- Primary Data Collection and questionnaire preparation

To meet the objectives of the study, both primary and secondary data have been collected. Semi-structured questionnaires have been constructed and administered to a sample of different stakeholders, including children, parents, technical experts and legal experts. To perform the quantitative or analytical study, research questionnaires have been prepared at first, where the questions are broadly divided into two types; demographic questions and descriptive questions. Noticeably, the demographic questions signify the personal constructs about the respondents. In contrast, descriptive questions intend to characterize or elaborate the respondents' perception or stakeholders towards the considered research variables such as scopes or opportunities and challenges for online child abuse.

The most natural tool Questionnaire is used for almost any instrument with questions or items to which individuals respond. Although the term is used interchangeably with “schedule,” it seems to be associated more with self-administered instruments that have items of the closed or fixed-alternative type (Kerlinger, 1973). Many published studies and numerous projects in education employ the instrument for data aggregation and accumulation. Characteristics of a good questionnaire were applied in designing the questionnaire for this study(Nworgu’s (1991), which includes relevance, consistency,

usability, clarity, and legibility. Questionnaires were designed to retrieve the key and essential information from the respondents on respective perspectives and perceptual experience towards online child exploitation and safety techniques involved to prevent online child abuse. Both demographic and descriptive attributes related questionnaires were prepared that exploited perceptions and suggestions of the different stakeholders. The overall questions were prepared as close-ended questions where demographic questions were framed as Yes, No, and multiple-choice type questions. The primary descriptive questions were prepared using a five-point Likert scale with multiple choices (options). In other words, to exploit more significant and generalizable outcomes, questionnaires were structured along a five-point Likert's scale encompassing labels as strongly agree (5), agree (4), neutral (3), disagree (2), and strongly disagree (1).

- Sample Population and sampling technique

The key specifications of the sampling population and the method (sampling) applied to collect responses and further analysis is discussed below. This study considers children who are the center point for the considered Region of Interest (ROI). Parents are undeniably responsible for monitoring internet use patterns of the children, their behavior assessment, and change assessment. Technical experts can help to identify the best possible technical measure to stop child exploitation or cyber-crime. Legal experts can help identify a possible inclusive approach to introducing web content filtering, pornography prohibiting measures, and inter-channel communication and supervision to stop child exploitation. The research considered children, parents, technical experts, and legal experts as the research population or sample population. Though this study focuses on assessing the issues mentioned above across India, the respondents have been considered from across the nation to inculcate diversity of responses based on one's demographic constructs. The inclusion of such diversity can help to enable justifiable or generalizable inference as the conclusion since children are the key stakeholder who often gets affected due to online stalking, cyber-trafficking, pornography. In this study, children have been considered stakeholders to get the internet use patterns, type of searches, type, and cases of online crimes or similar acts. Similarly, parents being the prime caretaker of the children, are also responsible for monitoring children's online behavior and internet use patterns. In addition, numerous

social behaviors can be detected easily at home that can signify a child's stress condition. Even parents are responsible for controlling internet use patterns at home. Considering these all factors, parents have been considered a stakeholder to participate in the case study. On the other hand, since this study intends to conceptualize or design a novel and robust filtering or control model for internet use by children, different technology experts, and legal experts have been considered. Here, technical experts are expected to suggest different measures to prevent online cyber-crimes and exploitation of or on children. It can help identify robust filtering or blocking concepts, content filtering, and verification before content access. On the other hand, legal experts can help identify suitable legal solutions to preserve children's rights by supporting filtering models or allied content filtering paradigms.

The respondents and their affinity to take part in the interview process are non-probabilistic. Hence, reaching random people and requesting them to provide expected responses can be the optimal approach. Observing the non-probabilistic scenario, where factors mentioned earlier, including accessibility and proximity, generally vary, the consideration of "Random Cum Convenience Sampling (RCS)" can be of paramount significance. Considering the general hypothesis or usual conception that convenience sampling might be biased, it should be noted that insignificant cases when data is collected through different online interactive platforms there can be replication or biasing probability. In this thesis, the "Random cum Convenience Sampling (RCS) method has been used as a sampling technique due to its effectiveness in the case when data is collected from different respondents or the different types of stakeholders having varied demographic features. Since this study, the personal semi-structured interview-based data collection has been done with the respondents, the probability of bias is alleviated. It, as a result, supports better diversity in response to generalize the research outcome.

- Data Analysis

Statistical Package for Social Sciences (SPSS), a well-known statistical tool, is used. Before analyzing the data, its reliability has been proposed to be assessed using the Chronbach Alpha method. The reliability test method can ensure whether the selected questions are reliable and consistent to give optimal inference. After confirming the reliability of the data collected, the data is analyzed using Comparative Mean, Mean

Plots, standard deviation, Factor analysis, independent sample t-test, and one-way ANOVA. Pearson correlation test is performed for the hypothesis test.

3.11.2 Systematic Survey

Literature survey is carried out with a focus on the approaches used globally, gaps in the approaches, differentiation of the problem, learning from other approaches to the current problem, similar approaches to the other problems, setting our work into context, avoid wasting efforts and checking for controversial results. Literature survey is identified as one of the methodologies in the entire research period. Based on literature and website survey classification of online activities leading to online(Kloess et al.,2014, Livingstone et al.,2014, Hadžović et al., 2015) and offline sexual abuse(Livingstone et al., 2014) against children were identified, and a review of online grooming and Internet-facilitated sexual exploitation of children was conducted.

Based on literature and website survey classification of intermediary vs. direct actors targeting children online was identified (Edwards 2010, CDT 2012). Actors involved in the Internet act as the intermediary and carry out different activities, including content uploading, hosting content, storing content, archiving content, cataloging content, and providing physical access to content as in Cyber Cafes. Internet is controlled directly or indirectly by intermediaries, making governments and law enforcement agencies gap in regulating Internet and cybercrimes.

3.11.3 Focus group creation for identifying technological readiness

Being the extensively used methodology of Information Systems research technique (Belanger, 2012), a focus group was used for collecting data with the interactive group participation on the topic identified and used for idea generation(Kitzinger 1995). Compared with face-to-face interviews, the focus group was expected to give comparatively better data regarding quality, reflecting from group members' views. A series of the focus group was formed for identifying technological readiness and experiment. The approach concentrated on the validation and refining of the proposed framework. The focus group discussion output was expected to be a comprehensive set of factors combining technical analysis and online safety framework readiness. Child online safety has been studied from many perspectives—technology use and selection, training and awareness, legal perspective, and policy development. Research and studies were carried out from a particular perspective rather than a holistic approach.

Focus groups were identified from Information Security professionals, academia, consultancy, law enforcement, and judiciary. A convenient cum random sampling approach has been used to collect responses from various stakeholders. Different stakeholders have been interviewed to assess respective concerns toward online child safety and other allied issues. As stated, the current study includes qualitative as well as quantitative approaches. The research approach considers descriptive and evaluative or analytical research paradigm to perform the intended study.

3.11.4 Case Study-Test lab creation for adult content identification

The technological growth is driving the predators to target the most vulnerable user base, children. Online child safety is identified as a global issue. Many countries have taken steps to battle child safety issues by introducing online child safety or protection-related acts. The promotion of child online safety applications and awareness programs has been initiated internationally. Lab setup provided a survey of various commercial and open-source electronic discovery applications, which shall cater to the identification of age-inappropriate contents in the form of image, text, video, keywords, documents, and Internet browsing history. The study provided a comparative analysis of the standard and unique technological features of various solutions. Based on the findings, an agent-based Client-server framework for adult content identification focusing on child safety in educational institutions is developed.

3.11.5 Case Study-Social Media Sentiment Analysis

Children initiate the usage of the Internet at a young age and spend more time online. Apart from the benefits like improved education, entertainment, news, and gaming, the Internet poses severe threats to children online. Ensuring online safety is a global challenge. Online social media responses and awareness posts on children's online safety were examined. In this relation, Twitter social media responses after freeing the accusers of children's sexual harassment and Facebook pages of some prominent personalities in India for online safety were analyzed. The results reveal that though the people are angry and fearful, they believe judiciary and police system and expecting safety from the same. The analysis of Facebook posts depicts that the concerned authorities are active towards online child safety and providing awareness through their representatives. People demand legal actions against the perpetrators of the crime to punish them. The current study is limited to Twitter and Facebook social media

platforms. The tweets are collected and analyzed concerning a single incident. Information posts are analyzed from a few personalities pages. In the future, the analysis can be extended to other social media, the tweets collected on multiple incidents, and information posts from more pages.

3.11.6 Case Study-Cyber Bullying detection Social Media text messages

Cyberbullying has become one of the significant problems in social media affecting teenagers. Efficient machine learning algorithms make bullying message detection possible. In this case study, deep learning techniques have been used for Cyberbullying classification based on the bullying content in the message. Convolutional neural networks (CNN) in the area of computer vision and speech recognition are well-known. A new model is proposed, which is a combination of CNN and Long short term memory (LSTM) and constructs a layer of bullying features set on the CNN-LSTM model. Twitter datasets were chosen, and pre-processing steps were applied. The result is applied to the CNN-LSTM model with the bullying feature set as the first layer. Nowadays, it is applied to the area of NLP applications also. The case study focuses on two approaches to deep learning. (i) CNN-LSTM with max-pool layer and (ii) CNN-LSTM without max-pool layer. The performance analysis is done for the proposed CNN-LSTM without a max-pooling layer with an accuracy of 94.41%.

3.11.7 Triangulation and recommendation

Triangulation is used as the research technique to corroborate various data inputs and validate the results for the agreement on the consistency of findings brought by different data gathering methods. As the final step, recommendations are made for improving online child safety in the Indian context.Fig.3.2 shows the proposed research flow chart.

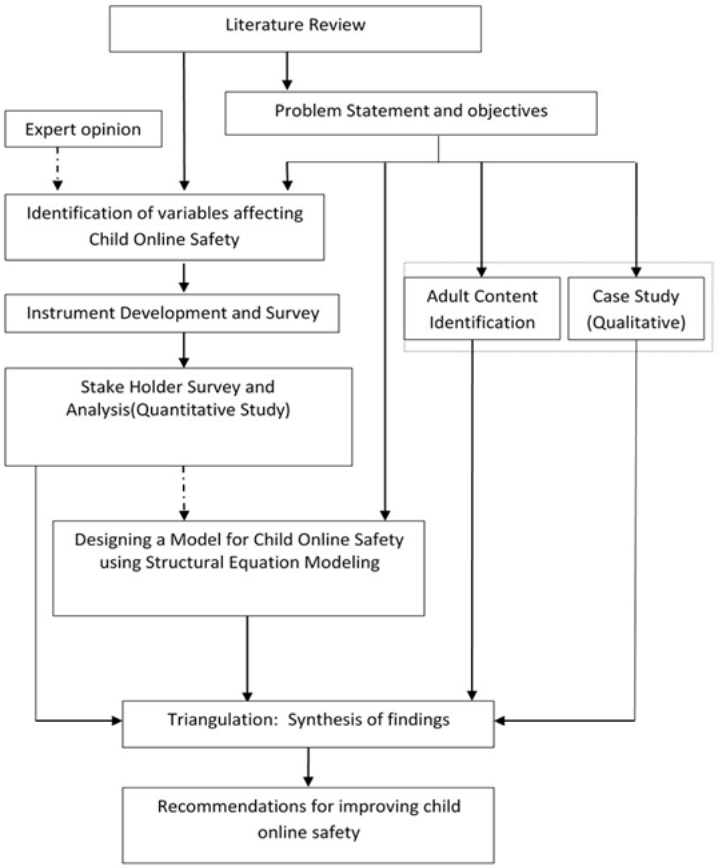

Figure 3.2: Research Flow Chart

3.12. Conclusion

The chapter presented the research questions and objectives, conceptual research model, and various methodologies. Various approaches such as research design, hypothesis formulation, data collection methods and the nature of data, tools implementation, and their implementation to accomplish overall research objectives were briefed in various sections of the presented thesis. The chapter discussed various research methodologies, associated constructs, and overall procedures. In the next chapter, case studies related to adult content identification, social media sentiment analysis, and cyberbullying detection in social media text messages are presented.

C H A P T E R 4

CASE STUDY

4.1. Introduction

The previous chapter described the methodological choices used in the current study. This chapter addresses three case studies in detail: (i) A Lab setup that provides test results of various commercial and open-source electronic discovery applications, which shall cater to the identification of age-inappropriate contents. (ii) Analysis of online social media responses and awareness posts on children's online safety (iii)Study on cyberbullying detection in social media text messages. The chapter is structured as follows. Section 4.2 describes the test lab setup, which provides a comparative analysis of standard and unique technological features of electronic discovery applications. Section 4.3 provides sentiment analysis of online social media responses and awareness posts on children's online safety from Twitter and Facebook platforms. A case study based on Cyberbullying detection in social media text messages and a model using a convolutional neural network and long short-term memory is discussed in Section 4.4. Finally, section 4.5 concludes the chapter.

4.2. Case Study I: Adult Content identification Framework -Test lab

In the current era of ICTs, where the Internet is widespread, children are not covered with a shield against overt sexual material, emotionally intense content, and elements including images or videos which are age-inappropriate. The technological growth is driving the predators to target the most vulnerable user base, children. Online child safety is identified as a global issue. Many countries have taken steps to battle child safety issues by introducing online child safety or protection-related acts. The promotion of child online safety applications and awareness programs has been initiated internationally. The case study focuses on a survey of various commercial and open-source electronic discovery applications, which shall cater to the identification of age-inappropriate contents in the form of image, text, and video, keywords, documents, and Internet browsing history. The study provides a comparative analysis of the standard and unique technological features of various solutions. Based on the findings, the research provides an agent-based Client-server framework for adult content identification focusing on child safety in educational institutions. The section can reference researchers and developers in adult content identification technology, implementers of the technology in academia, parents, and Law Enforcement agencies.

4.2.1. Adult content identification tools -characteristics and requirements

Pornography has been identified as significant cybercrime that negatively impacts children and teenagers (Adji et al., 2014). Identifying websites is essential for preventing the dissemination of adult or explicit content in the form of text, images, and videos. A combined method with technological, societal, and scientific approaches with regulatory law at national and international levels is essential for preventing the direct spreading and storage of such contents. From the technological perspective for ensuring the safety of children online, two propelling force areas for monitoring and examination have been identified. Firstly, Internet monitoring helps identify sites, determining the person who transgresses law by disseminating and restricting adult or explicit content (Sae-Bae et al., 2014). The second method directs attention to detecting such contents in computers, identifying keywords used in Internet searching and filenames, and examining active and deleted files (Sae-Bae et al., 2014; Pal and Memon, 2009). Both the technological methods require identifying adult content and commonly used keywords in an accurate and faster way. Advancement in storage capacity coupled with high internet bandwidth allows present-day computers to store millions of files in the form of images, videos, and documents that are illicit and abusive. Identification and analysis of such files and content is a difficult task. Many software solutions exist which shall provide features for the discovery of adult content with different features.

4.2.2. Overview of General Features of Adult Content Identification

- *Nudity detection in images and videos*

A tremendous amount of multimedia data available on the Internet has paved the way for attracting people to the Internet. Due to the lack of control, the Internet and World Wide Web have witnessed matchless pornographic content in images and videos. Image nudity detection has been established as the initial step towards identifying pornographic-related content (Santos et al., 2012). Adult image classification includes images of the nude body, images of erogenous parts of the body, and images having pornographic action (Xiaoyin et al., 2009). Nudity detection plays a major role in controlling access to age-inappropriate content (Rigan 2005). Video files are identified as a sequence of images, and each image is identified as a frame (Halsall,2001). Nudity

and pornography detection in videos are done using video frame extraction, motion pattern analysis, and audio analysis (Wang et al. 2004; Zuo et al. 2008; Jansohn 2009; Lopes et al., 2009). E-discovery tools open images and movies and scan for the presence of skin color. Skin tone analysis is used to identify images and movies that contain nudity and differentiate between normal images. While searching movies, each frame in the file is assessed for skin tone analysis. Generally, nudity detection prototypes require the extraction of image features, including skin color, texture, name of the file, image dimensions, the shape of the objects, and the identification of pertinent objects in the image.

- *Keyword scanning and document inspection*

Locating age-inappropriate and offensive content on computers or laptops is an essential feature of most adult content identification tools. Downloaded image files, movie files, and various other file types are searched in file names for obscene language and reflected content (Hyperdyne Software). Filename categorization is a particular case of short text categorization. The categorization is intended for recognizing pedophile media based on textual descriptions and typical expressions in the filenames that may contain pornographic keywords (Panchenko et al., 2013). A keyword analysis is expanded to identify obscene file content of text-based files and documents, including various formats like text, HTML, CSV, and document (Ho and Watters 2004). The search is generally carried against a list of known keywords, and results are being used to advance suspiciousness grading.

- *Web browsing history scanning and cookie analysis*

The web browser is a program that permits users to access web applications and web pages on the Internet. Information provided by web browsers is used to reconstruct online browsing behavior, including possession and distribution of child or illicit pornography and other adult content and improper use of Internet connection in conflict with the Acceptable Use Policy (Marrington et al. 2012). Web browsers are designed to record and retain much of the information related to user activities, including caching files, URLs visited, search terms, and cookies (Said et al., 2011). Web browsing history provides the list of web pages and associated data, including page title and time of visit. Browsing history can be used for identifying the visit to suspicious or adult content websites. Cookies are small sets of data sent from the visited website and stored in the

client system by the browser application, which helps remember stateful information and record browser activity. Scanning and analysis components check the Internet browsing history for offensive keywords and known adult websites. Generally, adult content identification solutions provide Internet usage details and the time of data access which shall provide the account of surfing details, including who, when, and where. Along with browsing history, cookies are also used by most adult content identification solutions for checking the presence of offensive or obscene words or phrases.

- *Compressed file scanning, file type identification, file extension checking, and renamed file identification*

Questionable content, including porn content in the form of images, movies, and documents, can be hidden as part of compressed file-formats including zip, rar, and similar other archive formats(Gubanov; Hyperdyne Software). Adult content identification software can open archive files and automatically identify unwanted material hidden, similar to routine operating system folder scanning. File extension gives the operating system the capability to identify the file and program need for opening the file. Solutions can identify and confirm the file type with the analysis at a binary level without depending upon the extension of files (Hyperdyne Software). Most solutions have the file type identification feature for scanning hidden files and renamed files by changing the extension and revealing the files' true individuality.

- *Safe file exclusion, review, and interactive deletion of detected offensive materials*

To improve the efficiency of scanning and analysis, a safe file list is created to include the attributes of files identified as safe. Files whose attributes are included in the safe file list are excluded from future scans, enabling the speeding up of scanning and helps the user to prevent from being included from further reviewing (Hyperdyne Software). Undesirable files and Internet search results detected can be reviewed periodically and added to a deletion list. Multiple view styles are provided for the detected content, including thumbnail view and text or tabular view. The Thumbnail view provides a small image of the detected content, which can be enlarged if needed and further audited. Text or tabular view provides file attributes, including filename, path, date of

creation, and suspiciousness level. After the review, identified files can be permanently deleted (Hyperdyne Software).

- *Logotype detection and warning text recognition in adult video*

Logotype superimposed in broadcasted videos is bringing some attention to the content of the videos, including the origination and genuinely of the content **(**Cózar et al. 2006; Cózar et al. 2007). Adult content detection products apply logotype detection used as a tool for automatic video cataloging system for examining the logos and the marking done by the porn studios used as a signal for identifying porn videos. As per law, legal porn studios are mandated to place a warning text at the beginning of videos to inform the viewing audience that the videos contain sexual scenes (Kuznech). Porn identification software compiles the list of keywords and key phrases used by pornographers to mark pornographic content.

- *Client-server architecture*

Enterprise-level adult content detection software scans servers, user profiles, and user storage areas for files and other attributes in a client-server architecture. Enterprise-level solutions can scan workstations across the network from a remote system with minimal impact on the host machines and users. Batch scanning at periodic time intervals can be scheduled over the network or identified workstation or group of workstations (Pinpoint).

4.2.3. Survey of tools- adult content identification and detection

Adult content identification software has various standard or unique features or capabilities, including porn detection in images, videos, and audios, file name analysis, web usage history analysis, and many more. An overview of available open-source and commercial tools available in the market will be provided in this section.

- ***Mediadetective***

Mediadetective (Media Detective) is commercial porn detection software, which scans the hard drives for any adult content and helps in cleaning it up. It features a file scanning engine that detects nudity and undesirable content in different file types. Scanning engine can find inappropriate video and image files by identifying different image formats including jpeg, gif, png, and bmp and various video formats like Avi, asf, Divx, Flv, ivf, Mpeg, qt, and mkv. A contextual parsing engine which is part of the detector, detects keywords and phrases in filenames and file content. The solution is to

scan and analyze in different file formats, including compressed file format, and ensure that no unwanted files are hidden. Evidence and details of adult website visits are identified with the help of Internet Explorer usage patterns by scanning the history files for keywords offensive in nature and known adult websites. Word document scanning facility checks for embedded images in the files. In addition, various other text formats are supported, including HTML and Cookie.

- ***Snitch plus and Pinpoint auditor***

Snitch Plus and Pinpoint Auditor are commercial tools from Hyperdyne Software which are well known for porn identification and removal (Hyperdyne Software). Snitch Plus provides features for automatic detection and removal of age-inappropriate material. It includes features for analyzing media files for nudity, identifying suspicious content in zip and other archived formats, an inspection of renamed files against file type using binary analysis, safe file exclusion for the previously identified safe files. Snitch Plus provides a facility for the review of internet usage history from browsers. Other features include cookie analysis and video formats evolved from mobile standards, keyword analysis, and Unicode support. Pinpoint Auditor is an enterprise version along with core features of Snitch Plus and allows scheduled and batch scanning across workstations.

- ***Kuznech adult content detection and filtering***

Kuznech Adult Content detection and filtering solution is a commercial tool that detects adult images and videos. It is based on skin detection, face search and recognition, logotype identification, warning text recognition, and scenes and objects classification with the help of convolutional neural networks(Kuznech; Smirnov et al.,2016).

- ***Content cleaner remove porn pro***

Content Cleaner Remove Porn Pro is a tool that allows the user to scan the computer for age-inappropriate content in categories including images, videos, Internet usage history, temporary internet files, cookies, and text files (Content Purity; Content Cleaner). The software uses an advanced skin-scan algorithm to detect images based on skin-tone analysis. Content Cleaner Remove Porn Pro will not block adult websites but clear away any trace of files saved on the computer. Content Cleaner has the capability for hidden and archived files and keyword search in filename and file content.

- ***Porn seer pro***

Porn Seer Pro is open source porn detection software that precisely identifies pornographic features in images and videos and generates patterns on illicit content, and provides the index for pornographic content for image or video databases. Porn Seer Pro detects specific features like breast, genital, vulvas, or other features on individual frames (Porn Seer Pro).

- ***Redlight***

Redlight pornography detection software developed by Digital Forensics and Cyber Security Centre, The University of Rhode Island, finds likely pornography content from images and videos(Digital Forensics and Cyber Security Center). The system uses image analysis techniques with extensive search criteria based on characteristics, including minimum and maximum file size, modification or access file attribute file headers, and file name type. Redlight can export hash sets of pornographic images in formats of well-known forensic tools, including EnCase, FTK, and X-ways.

- ***Smutsniffer***

Smutsniffer is a commercial solution that can scan computer storage media, including cache folders, download folders, TEMP folder locations, web browser history, and recycle bin and hidden folders or files for pornographic content in the form of images (Smut Sniffer). All the native image formats are searched, and images are analyzed for skin content. Movie formats are excluded from the search. The solution's capability is extended for providing legal documented facts, including hostname and IP address.

4.2.4. Comparative analysis

The feature-wise comparisons based on an empirical study of well-known Adult content identification software are summarized (Table 4.1). Features and capabilities including image analysis, video analysis, keyword search, document analysis, web usage history, file type, and name search, and enterprise architecture can be considered by the user groups and law enforcement agencies for the effective adult content or porn detection process and ensuring the safety of children while they are online.

Each software is having its advantages and unique features. Tools like Media detective, Snitch Plus, and Pinpoint Auditor are considering widely different feature sets, including Image Analysis, Video Analysis, Keyword search, Web Browser Analysis, File Type identification, File Extension Checking, and Compressed Folder Analysis.

Tools including Kuznech, Content Cleaner Pro, Porn Seer Pro, Redlight, and Smut Sniffer focus more on image and Video analysis with unique capabilities. Kuznech is using Logotype Identification and Warning Message Identification for the analysis of Porn videos. Pinpoint Auditor and Smutsniffer provide an enterprise architecture that allows applying the client-server model's electronic discovery features.

Table 4.1: Comparison of Adult Content Identification Software

Software/ Properties	Media Detective	Snitch Plus	Pinpoint Auditor	Kuznech	Content Cleaner	Porn SeerPro	Redlight	Smut Sniffer
Image Analysis	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Video Analysis	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Audio Analysis	No	Yes	Yes	No	No	No	No	No
Keyword search	Yes	Yes	Yes	Yes	Yes	No	No	Yes
Document Analysis	Yes	Yes	Yes	Yes	Yes	No	No	No
Web Browser Analysis	Yes	Yes	Yes	No	Yes	No	No	Yes
Compressed File Analysis	Yes	Yes	Yes	No	No	No	No	No
File Type Identification	Yes	Yes	Yes	No	No	No	No	Yes
File Extension Analysis	Yes	Yes	Yes	No	No	Yes	No	Yes
Renamed File Identification	Yes	Yes	Yes	No	No	No	No	No
Safe File Exclusion	Yes	Yes	Yes	No	No	No	No	No
Review of detected files	Yes	Yes	Yes	No	No	No	Yes	Yes
Logotype Identification	No	No	No	Yes	No	No	No	No
Warning Message Identification	No	No	No	Yes	No	No	No	No
Enterprise Architecture	No	No	Yes	No	No	No	No	Yes

4.2.5. Extended Framework and New Features

The present study shows that most of the tools under consideration are not conducting adult content identification from a forensic perspective. Current tools under the analysis are not adequate to identify adult or pornographic content from deleted files, temporary storage of data including clipboard data, recycle bin, and deleted browser history and cookies. Considering the mentioned drawback, we propose an agent-based Client-

Server model that Academia can directly implement to monitor student activities. The improved framework consists of an (i) Software Agent installed in the individual host over the network running in the background without any user interface; (ii)Server Software that the network administrator can use to view reports sent by the host machine. Agents are running periodically at specified time intervals depending on the search target, and reports are sent to the server system. The current framework emphasizes handling the identified features in the above discussions limited to Image Analysis, Video Analysis, Keyword Search including known websites, Web Browser Analysis including Internet usage History and cookies, File extension checking, File Type Identification, and Safe File exclusion, and Enterprise Client-server architecture. In addition to the comparative study's general characteristics, the framework has additional capabilities based on the search target, logging of search activity, and periodic automatic scan capability. When files are analyzed for the first time, hash values of the files are calculated and stored in the database. The file hash database stores the hash value of every file in the system and ensures that a file will not be considered twice for analysis, thereby increasing the performance. Novice features added to adult content detection software, and the architecture of the extended framework is presented in Figure 4.1.

- **Known content search using the hash database, URL list, and keywords**

Hash values referred to as digital fingerprints are strings of numbers and letters assigned to electronic data by a computer algorithm. Hash values are used in e-discovery to identify duplicate files and maintain the integrity of files for analysis. Hash values of known images and videos containing adult content are collected from online sources like Internet Watch Foundation and Virtual Task Force (Internet Watch Foundation; Virtual Global Taskforce). Hash values of newly downloaded and stored images and videos are compared against the hash database to identify adult content. Additionally, URL lists, keywords, and domain alerts are stored and indexed effectively in the database for effective matching. The automated scanning against the known content helps stop uploading or storing files in the system and protects children from repeat exploitation.

- **Recovery and analysis of deleted Internet history**

Internet history is stored in the Windows registry, and Internet cookies and recovery are made by targeting these two sources. Different mechanisms are used to recover internet history, including system restoration, cookie analysis, and access through log files (Oh et al., 2011). The model uses a system restore facility in a scheduled way for the recovery, which may lead to the reboot of the system. In addition, regular scans conducted periodically will inspect the DNS cache for finding the deleted history files between the last reboot and scan initiation time. The agent will scan browsing history and cookies to detect suspicious activities. A known website list is maintained in the server system as a CSV file. The current version of the prototype scans browsing data of Internet Explorer, Mozilla Firefox, and Google Chrome against keyword set and the website list.

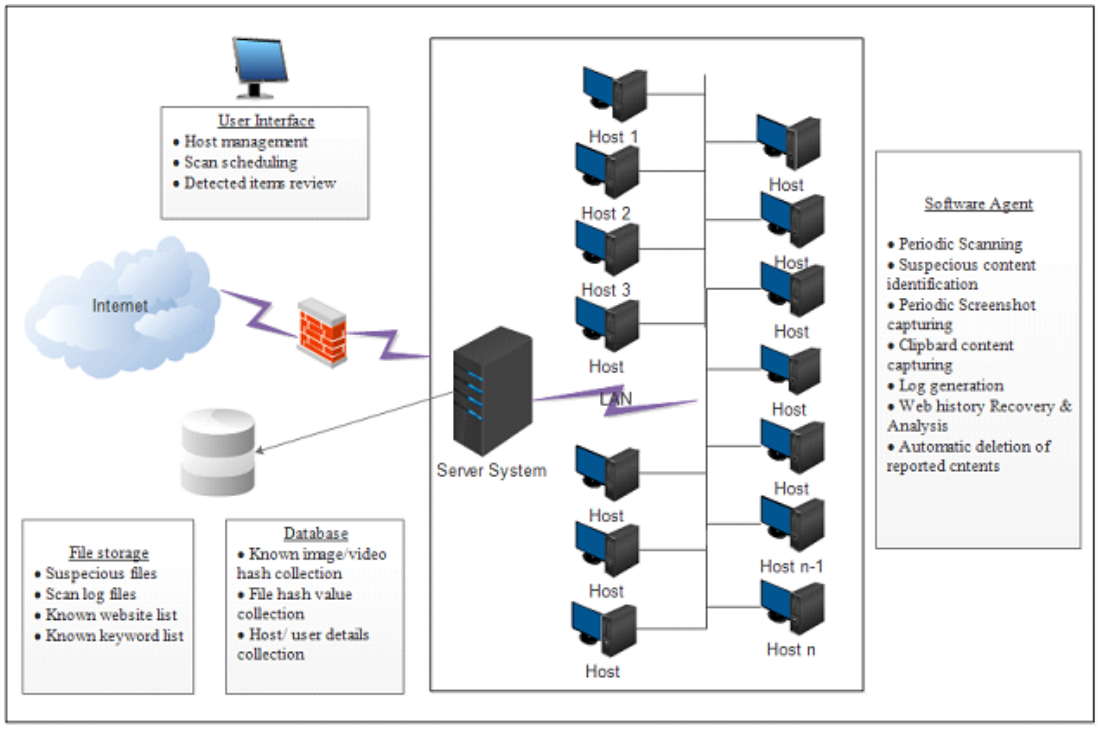

Figure 4.1: Architecure- Extended Framework

- **Periodic capturing of screenshot and clipboard content**

The model facilitates a manual review of screenshots and clipboard data for adult content identification from host machines. Screenshots are captured randomly from the hosts and saved in the server machine and a timestamp for manual analysis. Manual analysis of the screenshots will enable the administrators to find the websites being

browsed and applications being used by the host users. The additional module of the proposed system enables the capturing of clipboard contents to identify adult data. Clipboard may contain text data, images, pathnames, or URLs. Suppose the identified clipboard content is a pathname. In that case, the server will initiate a specific multimedia analysis or keyword analysis based on the type of file corresponding to the captured path. URLs identified in the clipboard will be compared against a known keyword. Clipboard analysis is made helpful in cases where files are copied from portable media to hard disk, hard disk to portable media, and from drive to drive.

- **Host management, Periodic scans, and Scan Logging**

The user interface in the server system acts as a dashboard where the administrator can add, remove and update host and user details in the network. Dashboard facilitates the review of identified files or content detected from various sources. Identified contents are filtered host-wise and user-wise with the tabular view and thumbnail view allowing opening the content directly for manual review. The scope of the dashboard is extended by the scan schedule facility provided to the administrator of the server system in addition to default scan settings. The scanning procedure is scheduled to start automatically on system startup. The agent will be running in the background without affecting other programs being executed in the host. Scan details are logged into a text file with details including hostname, username, scan time, and remarks corresponding to the scan activity. Logfile stored in the server is updated immediately after completing activities by the agents in various hosts.

4.2.6. Section Summary

The rapid growth of the Internet has paved the way for the proliferation of multimedia content. Adult content material, including images, videos, audios, and documents, is transmitted over the Internet, exploiting the high-speed connectivity and storage availability. The ease of access, anonymity and borderless nature of the internet has made it difficult to curtail the storage and distribution of adult content. From a technical standpoint, adult content detection, web browsing history, analysis of documents and files, and Internet monitoring are used to combat issues targeting children online. The section presented a survey of adult content identification solutions and their general characteristics and requirements. Based on the survey of existing tools and solutions, the section presented an agent-based Client-Server model. The proposed model

provides additional opportunities for effective adult content identification by including analysis of clipboard and screenshot, deleted browser history with an effective known content search using Hash database, URL list, and keywords from various Child Internet safety organizations and adult content reporting portals. The framework can be used for effective adult content identification in schools and controlled public places where children use the internet and computers. The framework proposed in the section can be scaled for deployment in various locations at national and international levels. The framework facilitates creating an adult content database including URL List, Keywords, Pornographic File Hash list, and Domain alerts that Law Enforcement can use Agencies, Government, Non-Governmental Organizations, and Academia.

4.3. Case Study II: Sentiment Analysis of Social Networking Applications in Indian Context

Children initiate the usage of the Internet at a young age and spend more time online. Apart from the benefits like improved education, entertainment, news, and gaming, the Internet poses severe threats to children online. Providing safety to children in online space is a global challenge. This section aims to examine online social media responses and awareness posts on children's online safety. People demand legal actions against the perpetrators of the crime to punish them. In this relation, Twitter social media responses after freeing the accusers of children sexual harassment and Facebook pages of some prominent personalities in India for online safety are analyzed. The results reveal that though the people are angry and fearful, they believe judiciary and police system and expecting safety from the same. The analysis of Facebook posts depicts that the concerned authorities are active towards online child safety and providing awareness through their representatives. The necessary actions should be taken for cybercrime awareness information to reach all social media users.

4.3.1. Background

Internet is gaining popularity in the life of children for their education and social development (Singh 2018). Children presently can access the Internet through mobile devices such as cellular phones, laptops, desktops, and other gadgets (UNICEF 2020). Like with the economy and society, the Internet is turning into a fundamental component of our kids' lives bringing benefits for their training, development, self-

articulation, and social progression(OECD, 2018; UNICEF, 2016). With a touch of a button, anybody can get access to information about anything around the world.

In recent years, Internet has allowed people to communicate with different parts of the world and acting as a gateway to the sea of information. Even though the Internet is considered an excellent tool for learning and access knowledge, the same tool exposes children to online threats and risks. These threats and risks impact the young minds of children negatively and compromise their online safety. With increased Internet availability, the risks may be severe in developing countries as it is difficult to manage online threats with limited resources(Dombrowski et al.,2007). Children share their personal information with strangers without knowing the consequences in the future (Whittle et al., 2013). There are various risks and threats on the Internet that encounter children and are divided into three groups: content, usage/conduct, and interaction/communication (LSE, 2015).

As the Internet penetration rises, risks pertaining to children on the Internet are rising, especially in developing countries like India. The resources are limited, and the capability to tackle such issues is complex(Singh, 2018). In recent years 2016, 2017, and 2018, the crimes against children in India are 106958, 129032, and 141764, respectively (Menon J, 2020). There are no boundaries in cyberspace. To combat online sexual abuse against children, international cooperation and assistance are essential. Therefore, the purpose of this section r is to examine online social media responses and awareness posts on children's online safety. In this relation, Twitter social media responses after freeing the accusers of children sexual harassment and Facebook pages of some prominent personalities for online safety are analyzed. The results are interpreted and recorded for policy suggestions.

4.3.2. Review of Related Work

With the development of the Internet and communication technology, it is easier to connect people from different parts. The Internet has provided new ways to enhance knowledge, skills, and participation to children and adolescents. These benefits are with the online cost risks to children such as bullying, grooming, sexual abuse, and hate content. The majority of the Indians will be connected to the Internet through mobile devices. India has the second-biggest mobile phone supporter base on the planet

(UNICEF,2020) because of moderate mobile phones and portable Internet bundles (Singh,2018).

The Internet is a medium that provides children with exceptional opportunities for overall development. For instance, the tools help children with disabilities to access different services and content from the Internet, which is challenging to access offline. Marginalized children with the membership of online communities can wider their identity and overcome online discrimination (Singh,2018). A survey conducted by the IAMAI of 35 Indian cities showed that about 28 million Internet users were school-going children out of 400 million Internet users. There has been an increase from 5% to 11% of Internet usage by children in rural internet access regions from 2014 to 2015. To be sure, the insurance of youngsters from online dangers and guaranteeing safe access to the Internet that will assist the children with developing their potential remains a significant priority.

Just as the flame has brought us warmth and light, the Internet has touched off a fervor for learning in a worldwide medium. Then again, as the dangerous power of the fire requires cautious utilization of this unusual component, the online association can open youth to a deceptive danger to their prosperity (Berson, 2003). For knowledge seeking and exchange, online technologies and mobile have brought many opportunities for pleasure and communication. Nevertheless, it does have side effects like cyberbullying, online sexual abuse, pornography. These exploitations are of significant concern for children(Livingstone et al., 2014). Cyberbullying uses electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. In India, part of article 67 in the IT Act is used to control cyber bullying (ITU, 2017). Cyberbullying may take the forms of grooming, emotional harassment, defamation and exposure, intimidation, and social exclusion(UNICEF 2020).

Online child abuse is a unique form of child abuse due to its virtual and distanced nature. For example, making unwanted sexual comments, uploading and creating images or videos of sexual abuse, and spreading it through social media can be considered online sexual abuse. Children may face this risk from the people whom they know and from strangers as well. Online abuse is supported by the Internet and may switch between online and offline modes. Online abuse may involve grooming a child by an adult online, abusing physically somewhere, and repeating online abuse by

sharing images of physical abuse. Sometimes, online abuse may occur only online by encouraging children to participate in online sexual activities(Mitchell et al., 2001).

If the children refuse to participate in future sexual activities, the abusers may create fear among the children, highlighting the conversation with the children's familiar persons (NSPCC, 2020). Irrespective of sexual exploitation, whether online or offline, the identification of the victims takes place online. Even though the sexual abuse carried is offline, "distribution, dissemination, importing, exporting, offering and selling" are the other forms of child online sexual exploitations (ECPAT,2020; Steel, 2015). In India, it is assumed that continuously being online and playing games may lead to addiction, resulting in attention deficiency. Studies observed the violent behavior with children after playing violent games (Ost, 2009; Lewin et al.,2009; Aboujaoude et al., 2015). This violent behavior maybe for a short duration. There is no direct relation between online presence and negative impacts on children but may create conflicts in the family (Kardefelt-Winther,2015).

Grooming refers to encouraging and preparing children for sexual abuse, violence, and illegal acts through sexual, religious, ideological, or other impactful conversations (Martellozzo, 2019; Wortley, R. and Smallbone, 2012). Based on the purpose of perpetrators and response from the children, these conversations may take a short or long duration. Grooming may be easily carried out on social media platforms if the victim considers the accuser as an online friend(Halder, D., & Jaishankar, 2014; barth et al., 2013; Aiken et al., 2011; Martin and Alaggia, 2013; McAlinden, 2012; Whittle et al., 2013) and other information shared by the children can be used to identify the behavior of the children(Gencer and Koc, 2012). The children can have public or private social media profiles; it is easier to trap them with public profiles.

4.3.3. Methodology

In the first part of the work, the data is collected from the Twitter platform after freeing the accusers of children's sexual harassment in the Southern part of India. The set of incident-related keywords are used to query Twitter social media. As a result of querying, the Twitter media provided a total of 1700 tweets. To know the insights of the Twitter content concerning punishment to the perpetrators of sexual violence, the collected tweets are analyzed in terms of emotions and sentiments. In the second part of the work, the posts related to children's online safety are collected from prominent

personalities on Facebook social media. These collected posts are analyzed manually to identify and understand mechanisms adopted to provide children online safety and their impacts. The results are interpreted and recorded accordingly.

4.3.4. Results and Discussion

4.3.4.1 Analysis of Twitter Content

In this section, the responses of online users against the release of accusers of children sexual harassment are analyzed, and the results are discussed. The analysis is made in terms of different emotions. The set of frequent words for each emotion from Twitter responses are shown in Figure 4.2.

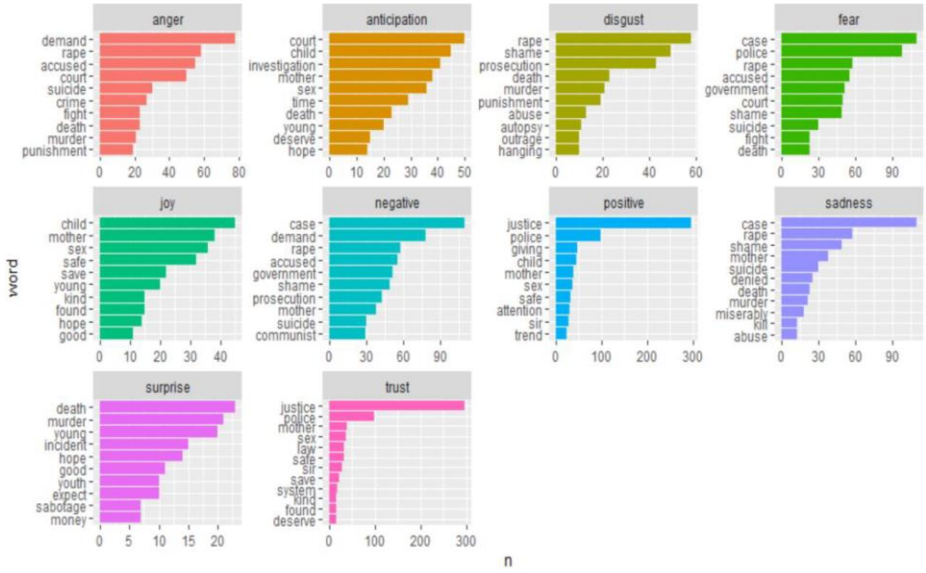

Figure 4.2: Emotions with Frequent Words

The terms “rape” and “death” occur with all the emotions anger, disgust, fear, and sadness associated with negativity. The words like abuse, suicide, punishment appear with more than one emotion. It indicates that people are unhappy with the incidents around them and demand punishment to the perpetrators involved in harmful incidents. The frequent occurrence of the words “justice” and “police” with the emotions trust and positive indicates that people have beliefs in the judiciary and policing systems of the country.

Different emotions and their coverage are shown in Figure 4.3. The radar graph reveals that the people are more worried and possess fear about the incident while expressing a similar amount of trust in the system to manage the situation. Similarly, people exhibit more anger, disgust, and sadness with the incident. The score for trust and anticipation

is more favorable among the positive emotions, whereas surprise and joy are more minor. It indicates that while trusting the system, they are expecting better from the system.

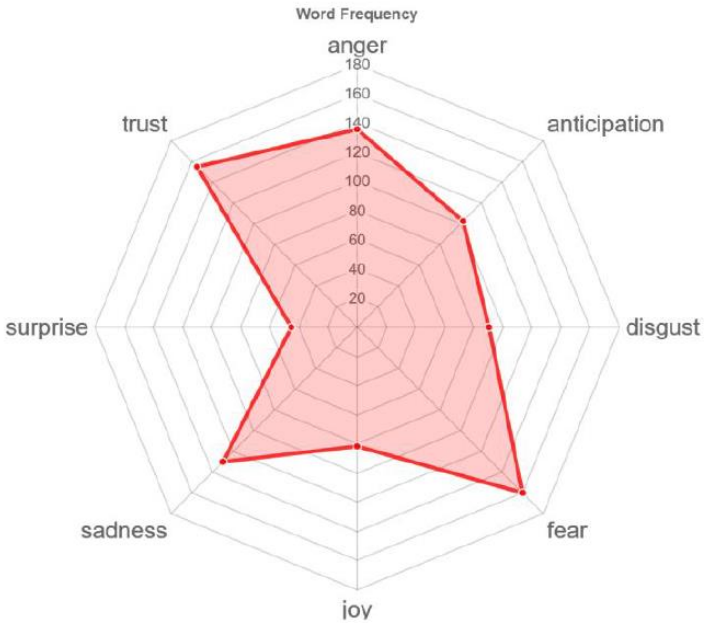

Figure 4.3: The Radar Graph of Emotions

4.3.4.2 Analysis of Facebook Posts

In this part of the work, the researcher analyzed some of the relevant Facebook pages of prominent personalities. Cyber-crime investigators contribute a lot to the online community by sharing the posts essential to cybersecurity and safety. The posts are in the form of images, videos, and texts. One of the posts shares the information on "how to deal with cyberbullying?". According to the post of the cyber-crime investigator, in case of online bullying, the victim has to follow the following steps.

Ignore it: This phrase conveys that if you undergo any cyberbullying, immediately neglect that message. If you respond, the perpetrators will continue bullying you online; otherwise, the perpetrators will stop bullying automatically after some time.

Block the person: If you are the frequent victim of a particular person by exposing to his/her messages, block that person from your list. This action in the future prevents you from seeing the posts from that person. In this way, you will be protecting yourself.

Tell someone: If you feared the incident, you share that with someone you trust, maybe your father, mother, brother, sister, or a close friend. This sharing will boost your morale and physical support to overcome the situation.

Keep a copy of evidence: Maintaining the proof of incidents is essential to fight against the perpetrators. Shreds of evidence strengthen the complaint against the offender of a cybercrime. The pieces of evidence may include text messages, e-mails, online conversions, and voicemails.

Report it: If you feel vulnerable to threats, report to the police department for action against the perpetrator. This action may protect you from being the victim of cybercrime as well as physical violence in the future.

This single post itself conveys many messages to online users on cybersecurity and safety. If every victim of cybercrime follows the steps, at the initial stage itself, the bullying can be mitigated easily. The problem associated with the post is its availability. As the post is shared among the friend's community, it will not be available to every Facebook user unless they try to access it. Though the post is of most importance for cyber safety, the post has been liked or commented on by very few members. There should be a provision to share these posts with all social media users for better performance.

In this relation, the Kerala Police created a social media profile on Facebook with the name "KeralaPoliceCyberdome." Under the banner of this unit, the authorities are organizing conferences and workshops in association with similar bodies to combat cybercrimes against children. The Cyberdome unit is working through the subunits such as the cyber awareness program (CAP) and BSafe by Cyberdome. The observation of the Facebook page of the unit reveals that the information posted on the page is receiving the average number of likes, shares, and comments comparatively. This may be due to an availability issue. As discussed earlier, this issue can be overcome by sharing the posts with all social media users, irrespective of their relationship with the unit.

4.3.5. Section Summary

The Internet is gaining popularity among children for the benefits of overall development. The benefits of the Internet make children compromise with cyber safety. In cyberspace, children are vulnerable to threats such as bullying, abuse, sexual abuse, sexting, grooming. The threats to children in the online world may be in the form of content, usage, and interaction. Though the crimes are taking place, people trust the judiciary and police system by anticipating safety in the future. People expect

punishment against the perpetrators of the crime. Several initiates are taken by governing authorities to combat cybercrimes. The representatives of the concerned units are trying their best to attain online safety for children. The necessary actions should be taken for cybercrime awareness information to reach all social media users. Some of the terms associated with positive emotions represent the actions against emotions associated with negativity. The popularity level of the posts on social media should be given importance. With the help of these insights, policymakers can design better policies to attain child online safety.

The current study is limited to Twitter and Facebook social media platforms. The tweets are collected and analyzed concerning a single incident. Information posts are analyzed from a few personalities pages. In the future, the analysis can be extended to other social media, the tweets collected on multiple incidents, and information posts from more pages.

4.4. Case Study III: Cyberbullying Detection in Social Media Text Messages

Cyberbullying has become one of the significant problems in social media affecting teenagers. Efficient machine learning algorithms make bullying message detection possible. In this section, the researcher used deep learning techniques for Cyberbullying classification based on the bullying content in the message. Convolutional neural networks (CNN) in the area of computer vision and speech recognition are well-known. A new model is proposed, which is a combination of CNN and Long short term memory (LSTM) and constructs a layer of bullying features set on the CNN-LSTM model. We choose the Twitter dataset and apply pre-processing steps to it. The result is applied to the CNN-LSTM model with the bullying feature set as the first layer. Nowadays, it is applied to the area of NLP applications also. This section focuses on two approaches in deep learning (i); CNN-LSTM with max-pool layer and(ii); CNN-LSTM without max-pool layer. The performance analysis of the proposed model is analyzed in terms of accuracy. In the proposed CNN-LSTM without the max-pooling layer, the accuracy is 94.41%.

4.4.1 Background

Cyberbullying is a type of bullying over digital devices like mobile phones, computers, and tablets. Cyberbullying occurs mainly through online social networking sites such

as Facebook and Twitter by sharing aggressive content with others. Sharing or sending these aggressive messages may affect the bullied person or victim negatively. The familiar places where it happens are Online Social Networking sites: Facebook, Twitter, Snapchat and Instagram, Text Messages, and Email(P.K Smith et al., 2008). Currently, we live in an era of the wide use of the Internet and ICT (Information and Communication Technology). Any content, including example photographs, text messages, posts, discussions, and remarks, can be shared through the Internet within seconds. Contents being shared by people are visible to anyone. The contents posted on the web – either their content or any harmful content – become an unchangeable open record of their perspectives and conduct. It can be thought of as online notoriety, which might be available to universities, schools, clubs, employers, and other people. It can easily hurt the people who are a part of it – the person being bullied as well as those doing the harassment. Sometimes it may not be easy to see the occurrence of cyberbullying. Teenagers are the most affected victims of cyberbullying attacks (Q Li, 2006).

Detection of cyberbullying from text messages using machine learning techniques are existing. The proposed system is based on a deep learning approach. It consists of the CNN-LSTM framework. The steps followed are preprocessing of text, word vector representation of messages, and classification. The embedding layer constructed with the bullying feature set is followed by the model's convolutional and LSTM layers. This model is used to show the accuracy of bullying detection.

4.4.2 Review of Related Work

An accuracy of 84% has been reported to be achieved when cyberbullying detection is applied on Twitter messages using SVM(Support Vector Machines), decision tree, and NBM(Naive Bayes Multinomial)in the Turkish language (UNICEF, 2016). In the case of Chinese text classification, different methods have been used, such as K-nearest neighbor (Q. Xu and Z. Liu, 2008), Support Vector Machine(S. Wei, J et al., 2013), Naïve Bayes (Z. Gong and T. Yu, 2010), decision tree (Johnson et al., 2010), and neural networks calculation (H. Zhuang,2017). Cyberbullying detection can be achieved in YouTube comments using different classifiers such as decision tree, Naive Bayes, and SVM(Dinakar et al.,2011). Detection of cyberbullying in Twitter can be carried out using sentiment analysis (Sanchez, and S. Kumar, 2011). The accuracy of bullying

detection can be increased by using information like age and gender (Dadvar et al., 2012). An improvement in cyberbullying detection is carried out using features that include the mean length of comments, capital letter usage, usage of emoticons, and the number of profane words(Dadvar et al., 2 013). Weighted TFIDF(Term Frequency-Inverse Document Frequency) for feature extraction and LIBSVM classifier is used to classify Slashdot, Kongregate, and Myspace (Nahar et al., 2013). The feature extraction technique helps to improve the performance of the LIBSVM classifier. CNN-LSTM framework is used for text classification (Hassan and Mahamood, 2018). Two models were described in their work: CNN –LSTM with max-pool layer and CNN-LSTM without max-pool layer. A pronunciation-based convolutional neural network for cyberbullying detection is available (Jamie and Edward, 2016). It used to do spell-check. It was evaluated on Formspring and Twitter datasets. An accuracy of 64% in Indonesian text messages for cyberbullying detection was achieved(Hani and Dade, 2018). Cyberbullying detection in Twitter messages using the semantics enhanced stacked denoising autoencoder method has been reported to achieve an accuracy of 84%(Rui Zhao and Kezhi Mao,2016).

4.4.3 Review of Related Work

Numerous techniques are present to classify the sentences, which use steps like pre-processing, feature extraction, and classification. The classifiers used for sentence classification are reviewed in the section.

4.4.3.1 Traditional Methods

- **Naïve Bayes Multinomial**

Naïve Bayes dates back to 1960's. It came into existence in the text retrieval community after 1960 and is mainly used for text categorization and identifying the category of documents, automatic medical diagnosis using word frequencies as features. It is based on the Bayes theorem with assumptions that are based on independence between the features.

- **Support Vector Machines**

Support vector machines (SVM) are mainly used in extreme cases. They precisely classify the data, compared to naïve Bayes-based techniques, and give less overfitting results. SVM looks for the extremes of the dataset and keeps a boundary known as a hyperplane. Different types of support vector machines are available in the literature.

A linear support vector machine (LSVM) separates data linearly. If the data is not linearly separable, we can not separate that data with a single line. In such cases, we can use non-linear support vector machines. It is one of the best techniques for binary classification.

- **K-nearest-neighbor classifier**

It is based on a distance matrix algorithm. Prediction of new instances class is made by finding the distance of the new one with existing training instances. Finally, we get a result of k instances with a lower distance to the new one. Based on the majority of class labels, it will assign the label for the new one.

- **Decision tree**

A decision tree that resembles a tree-like structure is used in the process of making decisions. It also depends on few more parameters like the probability of occurrence, cost of the resources, and utility. Conditional control statements are the only statements that are present in the decision tree. Operation Research is one of the areas where the decision tree concept is explicitly applied for decision analysis. A decision tree essentially consists of nodes and branches where nodes perform the test on the attribute while the branch indicates the test result. A leaf node is a class label, while the path can acquire classification rules from root to leaf.

- **Random Forest**

It is a straightforward machine learning technique. It is a group of decision trees, and it calculates and produces better results even without hyperparameter tuning. It generates several numbers decision trees and combines the results to get the final result. The random forest can be used for regression and classification tasks. It reduces the possibility of overfitting by the use of multiple decision trees. It efficiently works with large datasets and gives better accuracy.

4.4.3.2 Deep Learning Methods

- **Convolutional neural networks**

As of late, CNNs were connected to NLP frameworks and achieved exceptionally fascinating outcomes. Convolutional Neural networks are various layers of convolutions that can perform nonlinear operations; for example, tanh and ReLU are connected to the outcomes of each layer. These layers are like a sliding window over the input. It is known as an affine layer or a completely associated layer. It consists of

neurons in each layer with weight and bias. Each layer receives inputs and finds out the weighted sum, then forwards it to the activation function. In a traditional feed-forward neural system, each contribution of a neuron is joined to each yield in the following layer. In any case, Convolutional neural networks have distinctive methodologies. They are using the convolutions over the input layer to process the yield. Neighborhood associations figure the yield over the information layer, and after that, each layer applies distinctive portions, typically hundreds of filters, and then joins the outcomes.

- **Recurrent neural network**

It is a directed graph structure with nodes. These nodes are arranged into layers of RNN. Nodes in the current layer are connected with all the nodes in the following layer. Internal states of RNN are used to process the input sequence. The main idea of RNN is that it is using past calculations. Inputs are independent of each other in traditional neural systems. In traditional neural networks, all the inputs are independent of each other. Because of this advantage, RNN is applying to the areas like recognition of speech and handwriting. Long –short-term memory(LSTM) is a special type of RNN bit consisting of a cell, and a forget gate, an input gate, an output gate, and a memory state. A cell is a state where information is stored, and the gates control the information flow to the cell.

4.4.4 Existing System

Detection of cyberbullying from text messages using machine learning techniques involves the following tasks: pre-processing of text messages, feature extraction from the message, and classification. Pre-processing techniques involve mainly tokenization, stop word removal, stemming, and lemmatization. Then, features need to be extracted using TF-IDF (Term Frequency-Inverse Document Frequency) and Bag of Words (Bow). After that, classifiers like Naïve Bayes Multinomial, Support Vector Machines (SVM), Random Forest, k-Nearest Neighbors (kNN), the decision tree can be applied to demonstrate the accuracy of cyberbullying detection in text messages. Some deep learning approaches also can be used for the classification of text messages. The proposed model consists of only one convolutional layer and has a kernel size of 3 and 256 filters(Hassan and Mahamood,2018). It performs convolution on input data. The activation function is linear rectifier units (ReLU) within the convolutional layer. Only one layer of long short-term memory with the hidden state dimension of 128 filters is

used. Epoch is one forward and backward pass of the entire training set. Epochs are varying from 5 to 20 for training. Drop out is a regularization parameter, and it is applied between the convolutional layer and LSTM layer. Drop out is taken as 0.5. The above architecture with the max-pool layer is shown in Figure 4.4, and without the max-pool layer is shown in Figure 4.5. For text classification, it achieved an accuracy of 92%. Cyber-bullying detection based on semantic enhanced marginalized denoising auto-encoder has been described (Rui Zhao and Kezhi Mao, 2016). Initially, the authors constructed a bullying feature layer and taken it as a first layer. Following this layer, a marginalized denoising auto-encoder is used. It stacks some denoising autoencoders, and the result from each layer is concatenated and is taken as a learned representation.

4.4.5 The Proposed System

The various modules in the proposed system are training the dataset, Pre-processing, and classification, as shown in Figure 4.6.

a. Data Collection

Since no benchmark dataset is available, the researcher has taken the Twitter dataset, which contains messages that are labeled as bullied or not.

b. Pre-processing Steps

Data Pre-processing ensures that the dataset contains only the required information. The various stages in data preprocessing are as follows:

Tokenization

Tokenization is the way towards disseminating a vast arrangement of unstructured messages into a smaller subset of tokens. These are characterized by the assistance of different perspectives, such as blank areas, accentuation stamps sorted as expressions, and sentences.

- Before tokenization

  "I like you“
- After tokenization

  [‘I’, 'like', 'you']

Stop words Removal

The most widely recognized words utilized in a sentence such as ‘an’,’ 'will be,’ etc. These words do not make any sense but help in understanding the content. For example, before stop words removal, consider the sentence

['This', 'is', 'a', 'sample', 'sentence', ‘for’, 'checking', 'the', 'stop', 'words', 'removal',']. After stop words removal, it becomes [This', 'sample', 'sentence', ‘checking’, 'stop', 'words', ‘removal’, '.'].

Replacement of Special Characters

The strategy manages the substitution of unique characters like '@' with its correct word 'at.' In messages, this sequence has an enormous impact.

Stemming and Lemmatization

Porter Stemmer algorithm can be used to convert text into essential words(Willet, 2006). Lemmatization aims to give away dictionary form of a word using vocabulary and morphological analysis of words. It is a heuristic process that peels off the end of words and removes derivational affixes. It also detaches the inflectional endings. The words returned by the process of lemmatization are known as lemmas. For example, if we consider a token “saw.” Stemming may return only “s” while lemmatization may return “see” or “saw’’. The words which are returned depend on the way that the token is taken.

Transforming Case

In this step, all words in the messages are converted into lowercase. It is a crucial step because the same word in uppercase and lowercase may be interpreted differently. After these pre-processing steps dataset is divided into the training set, test set, and validation set.

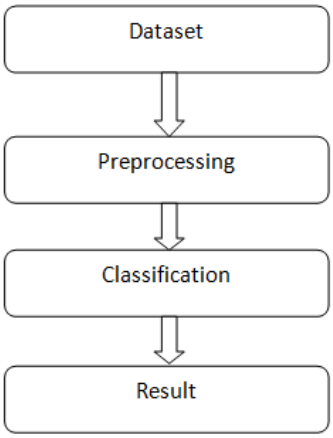

Figure 4.4: Flow Graph of the Proposed Architecture

c. Classification using Deep learning

Deep neural networks together execute feature extraction as well as classification. Here one hot representation is used to represent the sequence of words. Each word of the sequence is pointed into a continuous vector space. It is possible by multiplying with weight matrix, which gives continuous dense valued vectors. It is fed into a neural network model, which processes the sequence in various layers giving out prediction probabilities. This methodology is modified in order to maximize classification accuracy on the training set. Any assumption cannot be made about the word similarity using the one-hot vector. In any case, a one-hot vector makes no suspicion about the similitude of words. The model comprises CNN and RNN. The design utilizes word embeddings as data sources. This data is fed to CNN, which extracts features from it. The output is fed to the long short-term memory RNN model.

Construction of bullying feature set

It is imperative to create a bullying feature set above the CNN-LSTM model to improve cyberbullying detection. (a) The first step for constructing a bullying feature set is creating a list of dirty and negative words. We compare this list of words with the words in the messages. Then select the words present as expected in both. (b) The next step is to expand the list of predefined dirty words. It is based on word embeddings of the well-trained word2vec model. For this process, the corpus is converted into word2vec format, and that embedding is used. The cosine similarity of the words gives the semantic similarity between the words. Similar words are added to the list of dirty words, and the list of features can be improved. This feature set can be selected as the first layer of the proposed model.

Construction of other layers in the model

The model consists of only one convolutional layer and has a kernel size 3 and 64 filters that convolution input data. The activation function is linear rectifier units (ReLU) within the convolutional layer. Only one layer of long short-term memory with the hidden state dimension of 128 filters is used. Epochs is one forward and backward pass of the entire training set. Epochs are varying from3 to 5 for training. Drop out is taken as 0.1. Architecture with max-pool layer Figure 4.5 and without max-pool layer Figure 4.6 is constructed.

The main advantage of the convolutional layer is that it is used to extract higher-level features that are invariant to the local translation. It helps to extract the higher-level

features from the text messages. It needs multiple convolutional and pooling layers to get long-term dependencies. It becomes an issue when the length of the message grows. Instead of that, we can use a single convolutional layer with an LSTM layer. LSTM layer captures long-term dependencies. Most of the combinations like CNN-RNN models are applied to several types of pooling. The pooling layer retains the critical information and reduces the dimensionality and the number of parameters. There are chances of losing the long-term parameters.

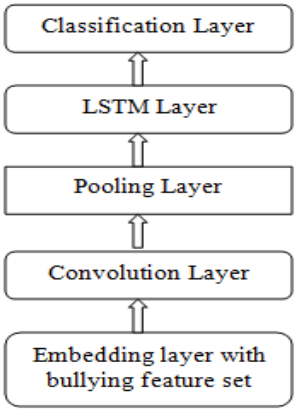

Figure 4.5: CNN- LSTM with a max-pool layer

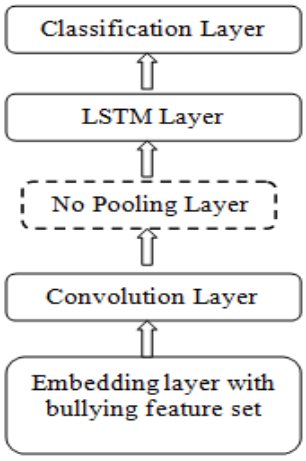

Figure 4.6: CNN- LSTM without a max-pool layer

4.4.6 Experimental Results

The performance analysis of the proposed model is analyzed by estimation of accuracy. Table 4.2 and Figure 4.7 show the results obtained by the traditional CNN-LSTM method. The method does not contain the bullying feature set layer. Both the methods CNN-LSTM with max-pool layer and without max-pool layer are compared. The

maximum accuracy achieved is 91.67% while using CNN-LSTM without the max-pool layer. The use of the max-pool layer is to reduce the feature map by reducing the dimensionality. It will increase efficiency.

Table 4.2: Accuracy Using Existing CNN-LSTM

Model	Accuracy
CNN-LSTM (without max-pool Layer)	91.67
CNN-LSTM (with max-pooling layer)	91.37

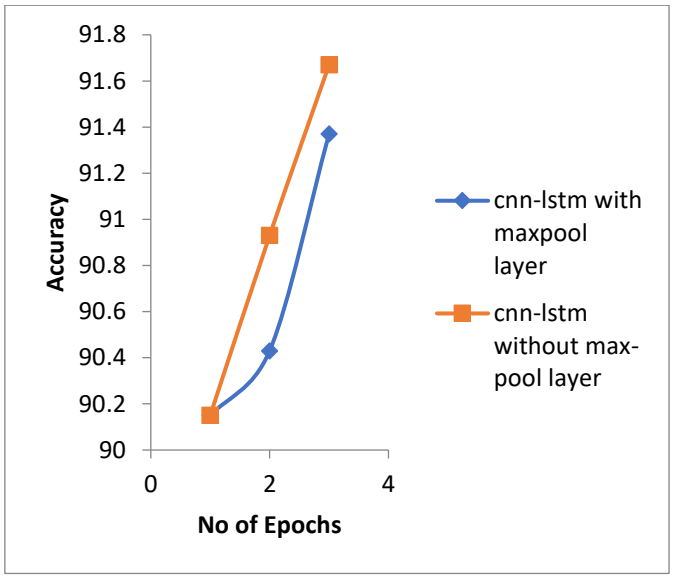

Figure 4.7: Accuracy Achieved using CNN- LSTM without bullying feature set

Table 4.3 and Figure 4.8 show the result obtained using the proposed CNN–LSTM model with the bullying feature set. CNN-LSTM model without using the max-pool layer achieves the highest accuracy of 94.41%, while CNN-LSTM with the max pool layer achieves an accuracy of 94.27%.

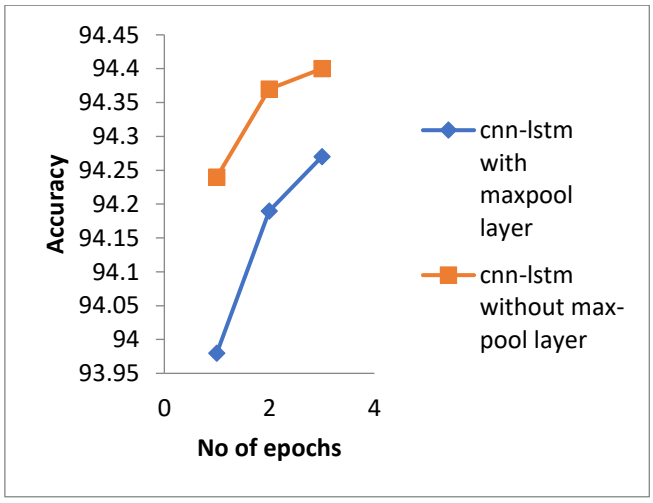

Figure 4.8: Accuracy Achieved using Proposed Model

Table 4.3: Accuracy Using Proposed CNN-LSTM with bullying Feature Set

Model	Accuracy
CNN-LSTM (without max-pool layer)	94.40
CNN-LSTM (with max-pool layer)	94.27

Figure 4.9 shows the comparison of proposed methods with the machine learning methods. Compared with machine learning methods such as NBM, J48(a decision tree), kNN, RF, SVM with linear kernel, and SVM with polygon kernel, results show that the proposed approach performs better than other approaches. Table 4.4 shows the accuracy achieved using machine learning methods. 91.42% accuracy is achieved by SVM with linear kernel. The accuracy increased by 3% when using the proposed CNN-LSTM without the max-pool layer.

Table 4.4: Accuracy Using Traditional Machine Learning Models

Model	Accuracy
NBM	91.19
J48	91.41
KNN	87.49
Random Forest	90.38
SVM-Linear	91.42
SVM-Polygon	89.75

4.4.7 Section Summary

A model using a convolutional neural network and long short-term memory is proposed. This model contains a bullying feature set as the first layer, followed by the convolution layer and LSTM layer. The proposed model is compared with the existing CNN-LSTM model for bullying text classification. Compared with the existing machine learning models, the proposed approach has shown better performance with CNN-LSTM without the max-pool layer.

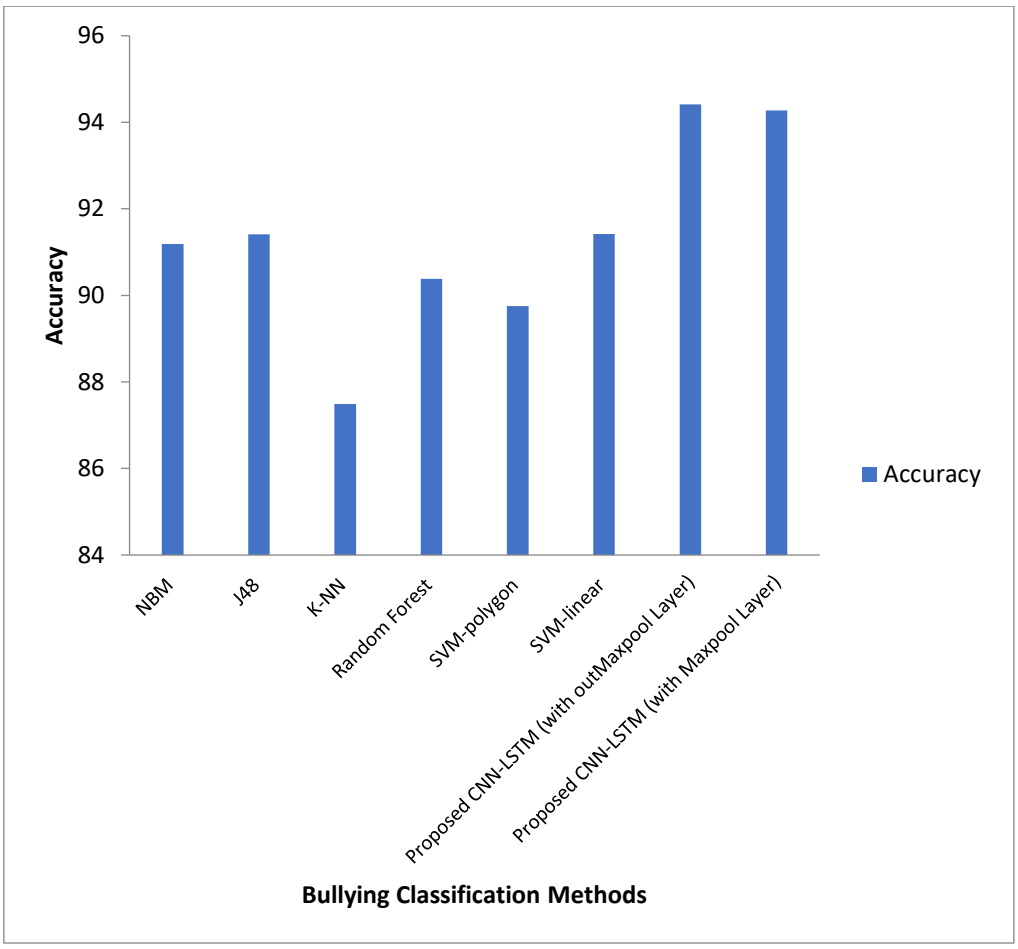

Figure 4.9: Accuracy Comparison of proposed methods with existing machine learning methods

4.5. Conclusion

The chapter discussed case studies related to adult content identification, social media sentiment analysis, and cyberbullying detection in social media text messages. Firstly the researcher described the test lab setup, which provides a comparative analysis of standard and unique technological features of electronic discovery applications. Secondly, the researcher presented a sentiment analysis of online social media responses and awareness posts on children's online safety from Twitter and Facebook platforms. Finally, a case study based on Cyberbullying detection in social media text messages and a model using a convolutional neural network and long short-term memory was discussed. The next chapter presents a quantitative analysis that provides the results of questionnaire surveys. Being multi-stakeholder research, analysis performed distinctly for various stakeholders Children, Parents, Technical experts, and Legal experts are discussed in the next chapter.

CHAPTER 5

QUANTITATIVE STUDY

5.1. Introduction

The chapter primarily discusses the data analysis and allied inferences. As already stated, being multi-stakeholder research, sections 5.2 to 5.10 of the chapter provides the analysis for each stakeholder -Children, Parents, Technical experts, and Legal experts. The analysis is performed distinctly in terms of demographic as well as descriptive components. The synthesis of the stakeholder survey is explained in section 5.11. Predictive analysis on parents' and technical experts' opinions is performed to test some of the hypotheses is given in section 5.12. Based on these identified variables, the different hypotheses on the prediction of parent and technical experts-initiated child online safety have been set. A detailed discussion of the data analysis and allied inference is given in the subsequent sections.

5.2. Quantitative Study- Stakeholder Survey and Analysis

Considering the exponentially up-surging rate of online child exploitation and harassment in the last few years, identifying specific inclusive preventive measures is of utmost significance. Understanding root causes, behavioral patterns, preferences and flexibilities, technical possibilities, and legal constraints can enable making an optimal and robust preventive measure to avoid online child exploitation in any form. These facts can be stated as the prime driving force and allied objective behind this empirical study. The principal goal of this research is to assess the perception of the different stakeholders, including children, teachers, parents, technical and legal experts, to understand root causes, behavioral perception, and possible solutions to avoid online cyber crime and (online) child exploitation. In addition, this research also intends to assess the efficacy of the different web-content filtering, risk-mitigation measures, and parental control paradigm to prevent online child exploitation cases in India.

Data Collection

To meet the objectives of the study, both primary and secondary data have been collected. Semi-structured questionnaires have been constructed and administered to a sample of students belonging to different age groups. The study has been targeted to be performed with a total sample of 600 respondents through a purposive stratified random sampling method. As mentioned previously, the study included children, parents, technical experts, and legal experts. For better illustration, the sample distribution of

the respondents has been discussed in the subsequent sections. A snippet of the data collection process and sources based on data nature is discussed in the subsequent sections. A snippet of the respondents and respective data size is given in Table 5.1. The questionnaire is given in Annexure II to V. As stated, 280 students or children were considered for an interview, while 220 parents were also interviewed in this study based on availability. As depicted in the table, the emphasis has been made on considering significant stakeholders in this study. It can help to conceptualize a novel and effective solution to prevent online child abuse. It can give more meaningful information pertaining to opportunities and current challenges in online child exploitation and various internet filtering techniques. A total of 50 respondents from each technical expert and legal expert were considered for further data collection.

Table 5.1: Distribution of the Respondents and Sample Size

SN.	**Respondents**	**Number of respondents**
1.	Children	280
2.	Parents	220
3.	Technical experts	50
4.	Legal experts	50
Total		600

5.3. Demographic Analysis for Children

In this section, a brief discussion of different factors motivating and facilitating the children to access online content has been discussed. Some of these demographic factors are gender, nationality, and age. A detailed discussion of each of these factors has been made in the subsequent sections.

Gender

Gender is one of the most significant factors in analyzing one's mindset. Undeniably, the gender of an individual influence his way of thinking, as it has been observed that both male and female have a different perspective towards the different tings taking place around them. Hence, for this research work knowing about the gender of children

is of paramount significance. Thus, the responses obtained to know about the gender of children involved in the study have been tabulated.

It can be observed from Table 5.2 that out of 280 respondents, 130 were male (46.4%), while 150 were female (53.6%). It can be inferred from the statistics that most of the respondents chosen for this study are females, while the males occupy a significant segment.

Age

Similar to gender, age is also an essential factor as it influences the maturity of the response obtained from an individual. In this section of the research work, the respondents' age has been enquired to know what ages of the children are accessing what type of content. The responses obtained for this question have been tabulated. It can be observed from Table 5.2 that 92 children (approximately 32.9%) were lying in the age group of 8-10 years, 87 children (31.1%) belonged to the age group of 10-12 years, 84 children (30%) were 12-15 years, and a small segment of the children (6.1%) were greater than 15 years. It can be observed from the statistics that the majority of the children belonged to the age group of 8-10 years while the second higher segment belonged to the age group of 10-12 years.

Table 5.2: Demography of Respondents- Children

Group item	**Gender/Age/Occupation**	**Respondent**	**Percentage**
Gender	Male	130	46.4
	Female	150	53.6
Age	8-10 years	92	32.9
	10-12 years	87	31.1
	12-15 years	84	30.0
	>15 years	17	6.1
Occupation	Student	122	43.6
	Joined schooling	124	44.3
	School drop out	24	8.6
	Uneducated	10	3.6

Occupation

The occupation of the children employed in this study is of paramount significance as it will enable an insight into the children's occupations, i.e., whether they are school-going and drop-outs. The variation in children's choice for accessing the content available online can also be identified through this question. The responses collected to identify the occupation of children have been tabulated.

It can be observed from Table 5.2 that 122 children (43.6%) were students, 124 (44.3%) had joined schooling, 24 children (8.6%) were school drop-outs, and a smaller segment, ten children (3.6%) were uneducated. The statistics plotted in the table depict that a higher segment of the respondents had joined schooling while the second-highest segment of the respondents is students. Interestingly, some students are not educated at all.

Parents' Occupation

Since accessing the internet or online content requires some multimedia device; hence it becomes necessary for this research to inquire about the parents' occupation to know whether they can access online content. Accessing online content is possible only when one has a proper internet facility and suitable devices. Also, it is noteworthy that such devices are not easy to afford for everyone. To obtain precise and appropriate results, the occupation of parents is divided into some categories. The responses collected have been shown occupation-wise in Table 5.3.

From table 5.3 it can be observed that 85 parents (30.4%) are employed, 108 parents (approximately 38.6%) told that they are self-employed, 20 parents (7.1%) are enrolled in some kind of studies and are hence students, 30 parents (10.7%) are unemployed, and 37 parents (13.2%) are involved in agriculture. It is noteworthy that only 10.7% of respondents are unemployed, and thus, their children can avail the devices required for accessing the online content.

The annual income of the family

In this section of the family's annual research income, the family has been enquired to know about the family's status. Also, through the annual income, whether the family earns well enough to provide better facilities to the child for his education and can arrange for additional necessities such as firewall, private tutor to guide the child. The responses collected for this aspect have been plotted in Table 5.3. It can be observed from Table 5.3 that 60 respondents (21.4%) told that their income lies in the range of

1-1.5 lacs, 91 respondents (32.5%) affirmed that their income lies in the range of 1.5-2 lacs, 48 respondents (approximately 17.1%) had their incomes in the range of 2-2.5 lacs, 58 respondents (near about 20.7%) had incomes in the range of 2.5-3 lacs, and 23 respondents (approximately 8.2%) had their incomes more than three lacs. It can be observed from the statistics that a majority of the respondents had their incomes in the range of 1.5-2 lacs, while the smallest segment of the respondents earned more than three lacs.

Place of residence

In this research, place of residence is considered an essential aspect because to access online content; the place where the individual is must have proper internet connectivity, and also it is noticeable that even in this digital era, the internet service providers are not able to provide their services in some villages and towns. This lack of service in these areas impacts the people residing there. Hence, to estimate the accessibility of the internet by children belonging to different places, here we have enquired about their places of residence. The responses collected for this aspect have been plotted in Table 5.3.

It can be noticed that a majority of the population of children lived in towns. It can be observed from the table that 46 children (16.4%) lived in the village, 151 children (53.9%) lived in town, and 83 children (29.6%) lived in cities. In contrast, the minuscule segment of the population lived in villages, showing that most children have access to the internet.

Size of the family

The size of the family is given significance in this research because through the size of the family, we can know about the number of children and adult members in the family. It should be noticed that the more the number of children in the family, the more will be sharing of ideas of about what to watch and what to not. Hence the responses collected to know about the size of the family have been shown in Table 5.3. It can be observed from Table 5.3 that 41 children (around 14.6%) said that they have1-2 members in their family, 93 children (33.2%) said that they have 2-4 members in their family, 88 children (31.4%) affirmed that have 4-6 members in their family and 58 children (20.7%) told that they have more than six members in their family. These

statistics showed that a majority of the children had 2-4 members in their family while the minuscule segment of the children told that they have 1-2 members in their family.

Table 5.3: Parents Background and Technology Information

Group item	**Individual item**	**Respondents**	**Percentage**
Parents' Occupation	Employed	85	30.4
	Self-employed	108	38.6
	Student	20	7.1
	Unemployed	30	10.7
	Agriculture	37	13.2
Annual incomes	1-1.5 lacs	60	21.4
	1.5-2 lacs	91	32.5
	2-2.5 lacs	48	17.1
	2.5-3 lacs	58	20.7
	>3Lacs	23	8.2
Place of residence	Village	46	16.4
	Town	151	53.9
	City	83	29.6
Family size	1-2 members	41	14.6
	2-4 members	93	33.2
	4-6 members	88	31.4
	Above 6	58	20.7
Residence type	Own house	147	52.5
	Rental	133	47.5
Technology awareness	Yes	150	53.6
	No	130	46.4
Social networking sites awareness	Yes	161	57.5
	No	119	42.5
E-learning tools awareness	Yes	162	57.9
	No	118	42.1
Frequency of using internet	Every day	140	50.0
	Sometimes	110	39.3
	Not at all	25	8.9
	Cant' say	5	1.8
The device used for accessing the internet	Computer	129	46.1
	Mobile	151	53.9
Usage of social networking site	Yes	183	65.4
	No	97	34.6
Influence by promotional ads	Yes	153	54.6
	No	127	45.4

Type of current residence

The type of residence of an individual refers to whether the person or living owns the house on rent. An individual living on rent might have a constraint on using or putting certain facilities such as Wi-Fi, playing loud music, and not allowed to go after a specific time while a person living in his own house can do whatever he wants. Hence here this aspect has been enquired to know the type of house a person is living in. The responses collected about this aspect have been shown in Table 5.3. It can be observed from the table that 147 children (52.5%) said that they have their own house while 133 children (approximately 47.5%) said that they live in rental houses. It can be observed from the statistics that the majority of the children lived in their own houses while a significant population lived in the rental houses.

Parents' awareness about internet technologies

The parents must be aware of the internet technologies existing in this era to help their children get the best education through online content and even keep a watch on them if they are going wrong somewhere. The response collected to know about parents' awareness towards internet technologies has been plotted in Table 5.3. From the data plotted in Table 5.3, it can be affirmed that 150 children (approximately 53.6%) said that their parents were aware of internet technologies. In contrast, a considerable segment, 130 children (46.4%) told that their parents are not aware of the internet technologies. It can be inferred from the statistics obtained that while a higher segment of the parents is aware of the internet technologies, most of them are not aware of it. It also exhibits that the lack of awareness about internet technologies can make parents lose control over what their children are doing when accessing online content.

Parents' awareness about social networking sites

Social networking sites are the most accessed by today's generation. They love to spend hours and hours on these sites. Also, the parents of children love to view such sites and chat or share pictures. However, sometimes such sites display poor content in videos, audios, or even pictures that children should not perceive. Hence, this depends upon the parents of these children whether they have sufficient knowledge about such sites or not and thus can prevent their children from accessing them. The responses obtained from the children about their parents' awareness of social networking sites have been shown in Table 5.3. It can be observed from Table 5.3 that 161 children (57.5%)

affirmed that their parents are aware of social networking sites, while 119 children (42.5%) told that their parents do not know social networking sites. It can be inferred from the table that a majority of the parents were aware of the social networking sites while a considerable segment lacked in having such awareness.

Parents' awareness about e-learning tools

The concept of e-learning is widely accepted by schools, teachers, students, and even parents to facilitate the best possible educational opportunities. However, there are still numerous individuals who are not aware of the benefits and drawbacks of e-learning. Among these individuals are some parents who are not aware of e-learning tools and prevent their children from using the online content for their studies. The responses collected to know about the awareness of parents about e-learning tools are tabulated in Table 5.3. The statistics obtained depict that 162 children (57.9%) said that their parents were aware of e-learning tools while 118 children (42.1%) said their parents were unaware of the e-learning tools. Interestingly, it is noteworthy that a majority of the parents were aware of the e-learning tools, but some were not aware of these tools.

Frequency of using internet

In the previous section, the responsibility for knowing about the population of respondents using the internet has been discussed, but the frequency of using the internet shall be identified. Since using the internet sometimes for fun is agreeable for children, using it for long hours and many times is not suitable for children. Hence it becomes necessary to know about the frequency of using the internet by children. The responses collected for this aspect have been tabulated in Table 5.3. The statistics obtained are interesting as it exhibits that most children use the internet almost every day while a very minute segment told that they do not use the internet. It can be observed from the data plotted in the table that 140 children (almost 50%) affirmed that they use the internet every day, 110 children (39.3%) told that they used it sometimes, 25 respondents (approximately 8.9%) stated that they do not use it at all. Five children (1.8%) said that they could not say how many times they used the internet in a day.

Device used for accessing the internet

Since this research deals with internet exploitation by children, it is necessary to identify the devices they use. While some children use laptops and PCs, the others use cell phones, tablets, i-pad. The responses obtained to know about the devices used by

children for accessing the internet have been plotted in Table 5.3. Interestingly, it can be affirmed that the statistics obtained depict that majority of children, 151(53.9%), used mobile phones for accessing the internet. In contrast, a lesser but considerable segment, 129 (46.1%), used computers for accessing the internet. It can be inferred from the statistics that mobile phones are the most common devices which allow children to use the internet. Hence, rather than restricting children from using the internet, their parents should take care that they do not use mobile phones much.

Social networking site

Social networking sites (SNS) are the most popular mediums of communication in the present world. They allow far distant people to connect, share their feelings and emotions. Hence, in the present era, social networking sites have become an inseparable part of human lives. Thus the responses to know about the use of social networking sites by children have been shown in Table 5.3. The statistics obtained here depict those 183 children (65.4%) affirmed that they use SNS while 97 (34.6%) stated that they do not use SNS.

Influence by promotional advertisements

Previously, a brief discussion of the use of social sites has been made. However, it is noteworthy that while accessing such sites, some promotional ads also on the sites sometimes act as traps and divert the focus of the individual. This diversion by promotional ads can sometimes be beneficial when they promote upcoming technologies while sometimes being harmful. These ads influence the user and attract him towards them. The responses collected to know about the influence of advertisements on the users have been tabulated in Table 5.3. It can be observed from the statistics obtained those 153 children (54.6%) affirmed that the promotional advertisements influence them, and 127 children (45.4%) said that the promotional advertisements do not influence them. The statistics obtained show that promotional advertisements influence a majority of the respondents.

5.4. Descriptive Analysis- Children

In the discussion, as mentioned earlier, critical factors associated with the demography of children have been analyzed. Hence, here a descriptive analysis of some other factors

associated with cybercrime prevention has been made. The results are obtained in the form of mean and standard deviation.

Purpose of using Internet

There are numerous purposes of using the internet, but these purposes vary from person to person. However, since this research work is entirely dedicated to preventing cybercrime by children, the purpose of using the internet needs to be accessed mandatorily to know the main reason for children accessing the internet. They also acknowledged these reasons to know how to mold children to access the right content and prevent them from indulging in any cybercrime. It is also noteworthy that the purpose of using or accessing the online content should be clear to the children so that they stay alert and aware of the unusual things occurring online. The responses collected to know about the reasons given by children for accessing the internet have been tabulated in Table 5.4.

Table 5.4 presents different reasons for which children are accessing the internet nowadays and multiple responses are given by respondents. Noticeably, 78% of children affirmed that they access the internet to share information with many people at once (M=3.81, S.D=1.035). They said that sometimes they get some vital information about their friends and group members and hence like to spread it to everyone as soon as possible, which is possible online with the help of online applications such as WhatsApp, Facebook, Instagram. However, the higher standard deviation depicts a wide variation in the responses obtained, and thus it can be concluded that not all children agree with the statement. On the other hand, approximately 82% of children said that their sole purpose of being online is to see videos and photos uploaded by their friends and other associates (M= 4.100, S.D=0.711). This segment of the respondents said that they enjoy viewing videos and photos posted by their friends, family members, relatives, and also it helps them stay connected with them. The standard deviation obtained also depicts that there is significantly less variation in the responses collected. Similarly, around 74% of respondents said they visit the internet or access online content to receive updates or comments (M=3.78, S.D=1.14). The respondents affirmed that receiving comments or updates about their pictures is significant for them, and they access online content to read these comments. However, the higher standard deviation exhibits a wide variation in the responses. A large population of the respondents, 80%

told that they enjoy viewing funny/entertaining videos/posts (M=4.00, S.D=0.78). The respondents said that the funny videos are a source of entertainment for them and help them relax their minds and refresh them. The respondents also affirmed that such videos help to stay more focused on their studies. A small but considerable segment of the population, 66%, said they access online content to stay updated with news and events (M=3.36, S.D=1.25).

Table 5.4: Purpose of Using Internet

Internet usage purpose	Mean	Std Dev.
Share the information with many people at once	3.8107	1.03517
Seeing photos / videos	4.1000	0.71140
Receiving updates or comments	3.7857	1.14714
Viewing funny/entertaining videos / posts.	4.0000	0.78972
Update with news & events	3.3679	1.25168
To Help/support others	4.1214	0.87962
To Get help/support from others	3.9571	0.97915
Receive feedback from others	4.0036	0.91776
To get news and updates about different products and services	2.6393	1.18619
To get daily socio-economic development news to make a better buying decision	3.9786	0.92336
Educational information or project-related information	4.1393	0.86668
It is significant supporting future academic accomplishments	3.2000	1.05884

However, not all respondents agreed with the statement. Interestingly, it should be noted that approximately 82% of respondents said that their main reason for staying online is to help others (M=4.12, S.D=0.879) while contrary to them near about 78% respondents told that they access online content to get help or support from others for their different problems (M=3.95, S.D=0.97). The respondents affirmed that they are familiar with many tips for different purposes that can be helpful for others, while the opposite segment told that they look for someone's excellent tips for their day-to-day problems. It is noteworthy that the standard deviation in both cases is lower and thus exhibits no disproportion in the responses obtained.

Some children, approximately 80% told that they wish to stay online to receive feedback from others (M=4.00, S.D=0.917). The respondents said they look forward to receiving feedback from others about their activities, photos. Some respondents also told that they get feedback from the online viewers about their questions, which helps them lower their curiosity levels and even find the solutions. A significantly lower population of the respondents, approximately 52%, asserted their main reason to use the internet or stay online to get news and updates about different products and services (M=2.63, S.D=1.186). The respondents said that, like the older adults, they do not get so much time to watch or listen to different news channels, and thus online websites serve as a source of news and updates for them about the trending pieces of stuff being available in the market. However, not all respondents agreed with the statement as depicted by the higher standard deviation.

Similarly, about 78% of respondents affirmed that staying online helps them get socio-economic development news to make a better buying decision (M=3.97, S.D=0.923). The respondents said that before buying any product, they go through its reviews and ratings online to buy the best product to fulfill their needs. They affirmed that news saves their time and helps them to make a better buying decisions.

Approximately 64% of respondents said they mainly use the internet to support future academic accomplishments (M=3.20, S.D=1.058). A considerable segment of the respondents, 82%, also said they visit online websites to obtain educational information or project-related information (M=4.13, S.D=0.866). The respondents affirmed that the projects and assignments assigned by their teachers are sometimes mind-boggling, and hence they require help from online websites. The respondents told that staying online also helps them in supporting their future academic accomplishments. They are told that they do not get relevant or desired information about their future aspirations and hence sometimes feel the lack of appropriate guidance, which is fulfilled through the internet up to a great extent.

Types of content

Undeniably, it can be affirmed that there is a wide variety of content available on the internet that serves different types of users. However, there is also a drawback of such a large volume and variety of content. It cannot be denied that though the content is helpful for different users, it has no restriction on the age of the users accessing it, which

sometimes proves harmful for minor age children. Hence, in this section, an attempt has been made to know about children's different types of content while viewing online websites. The responses obtained for this aspect have been plotted in Table 5.5.

It is noteworthy that approximately 86% of respondents told that they prefer to view blogs and bulletins available online (M=4.32, S.D=0820). They told that blogs and bulletins available online help them acquire out-of-the-box knowledge about the topic they desire. Hence, whenever they visit online websites, they review different blogs available. The lower standard deviation obtained also depicts that there is significantly less variation in the responses. About 58% of respondents said they preferred content where some community discussion occurred (M=2.94, S.D=1.11). The respondents said that such discussion keeps them updated about the changes in the community in which they live and even helps them build their knowledge about the allied issues.

However, it should be noticed that the standard deviation obtained for this aspect is higher, which signifies a wide variation in the responses collected. Some respondents, approximately 68%, said they preferred to view the profiles of different people and companies available online (M=3.43, S.D=0.877). The respondents said that this is a kind of hobby for them and apart from enjoying it they also get some knowledge about famous people and companies. They further added that such activities also add-on to their existing knowledge. Some respondents also told that they like to view their friends and relatives as it gives them enjoyment. The standard deviation obtained for this response is lower, and hence it can be estimated that most of the respondents agreed with the statement.

Contrary to the discussion mentioned above, some respondents, approximately 68%, said they prefer to view messages, chats type of content (M=3.45, S.D=0.902). The respondents affirmed that reading messages and chats are fun for them, and they enjoy these activities very much. About 80% of respondents said they prefer to access educational content online (M=4.04, S.D=0.727). This segment of the respondents asserted that accessing educational content available on the web is of great help. It is helpful for them in their day-to-day educational needs. They told that educational content available online, prepared by experts, sometimes serves as beneficial for their day-to-day school activities and provides them the extra guidance needed for their subjects. A large population of respondents agreed with this statement. Some

respondents, around 74% told that they like to surf music videos and audios available online (M=3.78, S.D=1.12). They told that music is a part of their soul and gives them immense pleasure to listen to such musical content. Additionally, they added that such musical content gives them pleasure and peace.

Table 5.5: Purpose of Using Internet

Group item	Individual item	Mean	Std. Dev.
Type of online content	Blog / Bulletins	4.3286	0.82038
	Community Discussion	2.9464	1.11071
	Profile	3.4393	0.87778
	Messages / Chat/Video calling	3.4500	0.90260
	Educational resource access	4.0429	0.72706
	Music	3.7893	1.12732
	Events	3.7214	1.14578
	Tweet / Comment	3.6286	1.16915
	Grab / Copy / share	3.8107	1.03517
	Forums / Groups	4.1000	0.71140
	Videos	3.7857	1.14714
Need of online content	It enables socializing irrespective of location and other demographic constructs across the world	4.0000	.78972
	It helps in getting information about subject-matters (Educational)	3.3714	1.24632
	It helps in making better carrier decisions and reviews.	4.1321	.82112
	It helps in knowing the world and activities better.	3.9571	.97915
	Internet facility helps students in getting more suitable and significant e-learning contents.	3.9571	.97915
	It helps in getting education & personality development approaches	3.3607	1.15248
	Social media helps the students to do their assignments, projects, and other relevant information.	3.8071	1.04998

A similar population of the respondents also said they preferred the content related to events (M=3.72, S.D=1.14). The respondents said they are curious to know about the different events in the world and wish to know about them. Hence, they like to perceive such content available online. A slightly lesser population of the respondents said they like to go through tweets and comments posted online (M=3.62, S.D=1.16). The

respondents told that going through such comments is sometimes enjoyable and sometimes inspiring for them. Contradicting them, some respondents told that reading such type of content is a wastage of time, and hence it should be noted that the standard deviation obtained for this response is higher.

Interestingly, it has been observed from the responses obtained that 76% of respondents told that they prefer the content that can be copied, shared, and grabbed (M=3.81, S.D=1.03). The respondents asserted that they like to share some content with their friends, relatives and hence prefer the content that can be shared and copied. Approximately 82% of respondents said they preferred to view forums or groups (M=4.10, S.D=0.71). The respondents said that such content serves as a source of knowledge for them, and they find it more interesting than any other content available online. They are sometimes told that such type of content allows them to connect with other people.

On the other hand, some respondents, near about 74%, said they prefer videos available online (M=3.78, S.D=1.14). This segment of the respondents told that the videos available online help them for different purposes and even impart knowledge about various topics. They also added that such videos sometimes provide them fun and amusement too.

Need of online content

Online content is nowadays beneficial for users of different domains and segments. It helps them acquire extra knowledge and information from the experts and sometimes even motivates them to perform better. We have collected their responses to know about children's opinions towards the need for online content in this section. The responses obtained are plotted in Table 5.5. Interestingly, it should be noted that approximately 80% of respondents told that online content is necessary since it enables socializing irrespective of location and other demographic constructs across the world (M=4.00, S.D=0.789). The respondents said that most online sites facilitate socialization among its users by providing answers to the questions posted on the sites and allowing them to communicate with each other. Contrary to this, about 66% of respondents said that online content is necessary as it helps get information about subject matters (M=3.37, S.D=1.24).

The respondents added that online content is available on different subject matters (educational), allowing users to learn about their subjects and clarify their doubts. The respondents told that such information provided by subject experts sometimes imparts in-depth knowledge of the concepts printed in their books. 82% asserted that the online content helps them make them better carrier decisions and reviews (M= 4.13, S.D= 0.82). This segment of the respondents said that nowadays, there are such excellent websites that provide counseling to children and guide them towards making a better carrier decision that was previously not there. The children said that such advancements had benefitted numerous children whom they or any of their family members did not know about the carrier options.

A few respondents were approximately 68% told that the online content helps them know the world and activities better (M=3.95, S.D=0.979). The respondents told that nowadays, there are so many facts and information available on the web that children can quickly grab sufficient knowledge about the world and allied activities. They also added that such information helps them to stay ahead of their competitors. A similar population of the respondents also told that internet facility helps students in getting more suitable and significant e-learning contents (M=3.95, S.D=0.979). The respondents asserted that the wide range of content available on the web helps students by providing significant e-learning content that is sometimes not provided by the schools or the videos shown to demonstrate concepts. They added that the online content sometimes proves a boon for them and removes the myths existing in their brains. The standard deviation obtained from this response is also lower and hence demonstrates that there is not much variation in the responses.

Approximately 66% of respondents said that online content helps get education and personality development approaches (M=3.36, S.D=1.15). The respondents said that, as discussed previously, some websites facilitate experts' opinions for children searching for guidance for their educational needs and even guide for some personality development approaches that can be helpful for them in the future. Similarly, about 76% of respondents told that social media helps students do their assignments, projects, and other relevant information (M=3.80, S.D=1.04). The respondents revealed that the educational material available online gives ideas about the assignments, projects and helps to create innovative projects and thus obtain good scores.

Need of cybercrime avoidance measures

Cybercrime has been impacting many people's personal and professional lives, among which the most significant ones that are harmed are children. It is so because children are the ones who can be trapped easily as they provide their information very quickly and without considering the risks hidden behind it. Hence, it is of paramount significance that some strong cybercrime avoidance measures should be initiated to prevent innocent children from being trapped and harmed by hackers. The responses gathered towards knowing the reasons for the need for cybercrime avoidance measures have been plotted in Table 5.6. While discussing the issue of cybercrime with the children, it was found that 66% of respondents told that cybercrime avoidance solutions could help in preserving personal details (M=3.36, S.D=1.32). The respondents asserted that due to escalation in cybercrime, they observed growth in stealing personal details of online users. The respondents said that leakage of such details could harm online users and sometimes can even create mental pressure and stress. Approximately 56% of respondents said cybercrime avoidance measures could help children avoid suspicious activities of contents affecting moral and social nature (M=2.85, S.D=1.11). Some children said that such measures would block specific sites that are harmful in any aspect and thus help children be away from such sites.

Possible cybercrime avoidance measures

As discussed in the previous sections, most respondents have asserted an urgent need for cybercrime avoidance measures to protect the users, especially children visiting or accessing online sites. In order to know about the response of respondents towards some possible cybercrime avoidance measures, in this section, a brief discussion of the cybercrime avoidance measures has been made. The responses gathered for this aspect have been plotted in Table 5.6.

It can be observed from Table 5.6 that approximately 60% of respondents told that providing limited access time to children is one of the best possible measures that can be implemented (M=3.03, S.D=1.22). The respondents revealed that by limiting the time to access the internet, children would access only the required sites or the ones that need most or enjoy most. In other words, they will not be to access unnecessary content existing on the online websites and thus will not be providing their personal information on any and every website. On the other hand, approximately 74% asserted that

implementing advanced content filtering techniques can be an optimal measure to prevent cybercrime (M=3.77, S.D=1.19). The respondents stated that by implementing advanced content filtering techniques, the users would view only those significant or valuable content for them and prevent them from accessing the other content that is not meant for them. The respondents also added that parents would control children's activities through filtering techniques without any direct interruption. Like the aforementioned discussed aspect, nearly 76% of respondents affirmed that demographic variable-based content filtering is significant for preventing users from cybercrime (M=3.82, S.D=1.04). The respondents replied that by applying filters based on demographic variables such as age and gender, the users could access content suitable for them and even published online, especially for people of their age. They added that this will allow people of a particular age to access the content according to their age and will not allow them to view unnecessary content that is not significant.

Interestingly, approximately 68% of respondents said that log-based parental control and auto information exchange are the best measures to prevent cybercrime (M=3.46, S.D=1.10). The respondents told that log-based parental control allows the system to store the data about the websites searched by the user so that the system administrator can view it anytime and track the content searched or used and thus prevent the user from being harassed or cheated. The respondents also affirmed that auto information exchange is another suitable measure that can limit cybercrime. The respondents said that this technique facilitates the exchange of information to the parents and teachers about the user's content and thus allows them to control the user.

A small yet considerable segment of the respondents, approximately 64%, told that cyber counseling is the best measure for preventing cybercrime (M=3.23, S.D=1.30). The respondents stated that counseling the users about good and bad content existing on the internet can prevent them from facing any issue allied with cybercrime. They added that the users should be explained the significance of their personal information and thus the impact of leaking it to an unknown person. Additionally, the users told that the generation nowadays is brilliant and is capable enough to understand the concept of right and wrong and hence should be provided cyber counseling through different mediums such as books, games, or acts. Approximately 76% of respondents told that user-centric log-analysis and information exchange could be a possible cybercrime

avoidance measure (M=3.81, S.D=1.03). The respondents said that through the approaches such as information exchange, it becomes easier to monitor the sites searched by kids and thus control their activities by employing a firewall or limiting their time accessing the internet. Some respondents also said that by analyzing the log information, they could also find out the websites searched by their children and thus make some efforts towards controlling their activities.

Table 5.6: Need and Possible Measures of Cyber Crime Avoidance

Group item	Individual item	Mean	Std. Dev.
Need to avoid cybercrime	Cybercrime avoidance solutions can help in preserving personal details	3.3643	1.32368
	It can help children to be away from suspicious activities or contents affecting moral as well as social nature	2.8500	1.11313
Measures to avoid cybercrime	Limited access time to the children	3.0357	1.22934
	Advanced content filtering	3.7714	1.19042
	Demographic variable based (age/gender) content filleting	3.8286	1.04345
	Log-based parental control and auto-information exchange	3.4679	1.10669
	Cybercounseling	3.2393	1.30476
	User-centric log-analysis and information exchange	3.8107	1.03517
	Access denial to the in-system memory space or data	4.1000	0.71140
	Pre-audit of the mobile applications as well as websites for transparent service provision	3.7857	1.14714

A significantly larger population of the respondents, approximately 82%, told that denying access to in-system memory space or data can be a potential measure to avoid cybercrime (M=4.10, S.D=0.711). The respondents said that denying access to in-system memory can prevent personal information leakage and thus prevent data misuse. They added that denying such access can prevent their children from visiting or downloading any malicious content. It is noteworthy that the lower standard deviation signifies that most of the respondents agreed with the responses, and hence there is not much variation in the responses obtained. Approximately 74% of respondents said that pre-audit of the mobile applications and websites for transparent service provision

could be an effective measure (M=3.78, S.D=1.14). The respondents said that by pre-auditing the mobile applications and websites, the children are accessing the right content. They added that performing such measures can enable them to know about the contents published on the sites and thus prohibit or advise their children not to access such content. However, the higher standard deviation signifies a much variation in the responses obtained; hence not many respondents agree with the statement.

5.5. Demographic Analysis for Parents

In the previous section, children's views towards cybercrime and the need for measures to control cybercrime escalation have been discussed. Children's perspective has been explored fully; however, it is of paramount significance that parents' perception is also discussed. Thus, in this section, the demographic constructs of parents have been considered significant, and a brief discussion is made.

Gender

Gender has always been a dominating factor in any research work. It is because the gender of any individual determines his thoughts and opinions towards a particular aspect. In other words, gender reflects the mindset of an individual and defines his assertions for something. The responses collected to know about the gender of the respondents have been plotted in Table 5.7. It can be observed from the table that 130 respondents, 59.1%, were male while 90 respondents, 40.9%, were females. It can be observed that a majority of the respondents who enquired about this study were males. However, a considerable segment of females was also considered.

Age

Apart from gender, age has also been considered a significant factor for this research because an individual's age demonstrates how he answers the questions and even the appropriateness or preciseness of his answers. In order to obtain accurate results, the age of the respondents has been categorized into different groups. The responses collected have been plotted in Table 5.7. It can be observed from the table that 13 respondents, 5.9% belonged to the age group of 20-30 years, 89 respondents, approximately 40.5% belonged to the age group of 30-40 years, 101 respondents, near about 45.9% belonged to the age group of 40-50 years and 17 respondents, approximately 7.7% were more than 50 years in age. It can be observed that a majority

of the respondents belonged to the age group of 30-40 years and 40-50 years, and a minuscule segment of the respondents belonged to the age group of 20-30 years.

Table 5.7: Demography of Respondents- Parents

Group item	Gender/Age/Occupation	Respondent	Percentage
Gender	Male	130	59.1
	Female	90	40.9
Age	20-30 years	13	5.9
	30-40 years	89	40.5
	40-50 years	101	45.9
	>50 years	17	7.7
Occupation	Employed	85	38.6
	Self-employed	105	47.7
	Student	12	5.5
	Unemployed	7	3.2
	Agriculture	11	5.0
Annual income	1.5-2 lacs	24	10.9
	2-2.5 lacs	57	25.9
	2.5-3 lacs	79	35.9
	>3Lacs	60	27.3
Place of residence	Village	18	8.2
	Town	92	41.8
	City	110	50.0
Family size	1-2 members	12	5.5
	2-4 members	148	67.3
	3-6 members	60	27.3
Current residence	Own house	172	78.2
	Rental	48	21.8

Occupation

An individual's occupation is considered a significant aspect for this research because occupation symbolizes the potential of an individual to avail the luxuries or, in standard terms, fulfill the necessities of life. In this research work, the occupation has been categorized into five different segments. The responses collected to know about the occupation of respondents have been tabulated in Table 5.7. It can be observed from the table that 85 respondents, 38.6% were employed at some organizations, 105 respondents, 47.7% were self-employed or, in other words, had their businesses, seven respondents, 3.2% were unemployed and 11 respondents, 5% were enrolled in agriculture. It can be inferred from the statistics obtained that a majority of the respondents were self-employed while a considerable segment was enrolled in agriculture also.

Annual incomes

As discussed previously, an individual's occupation reflects the potential of an individual to fulfill his necessities. Similarly, income can be defined as the earnings of an individual from his occupation. Both occupation and income together form the socio-economic status of an individual. These two aspects are of paramount significance for this research as they can help determine whether an individual can fulfill his child's additional needs, such as laptops and smartphones. The responses gathered to know about this aspect have been plotted in Table 5.7. It can be observed from the data plotted in Table 5.7that 24 respondents, 10.9% earned in the range of 1.5-2 lacs, 57 respondents, 25.9% earned in the range of 2-2.5 lacs, 79 respondents, approximately 35.9% earned in the range of 2.5-3 lacs and 60 respondents, 27.3 % earned more than three lacs. It can be inferred from the responses obtained that the majority of the respondents earned in the range of 2.5-3 lacs while a smaller segment of the respondents earned in the range of 1.5-2 lacs.

Place of residence

In this research workplace of residence of an individual holds a special significance since the research deals with cybercrime, for which the internet is a necessity. Undeniably, not all individuals are located in cities; some are located in towns and villages. Hence, to identify the cumulative strength of cybercrime, people residing in different places must be involved in research. The responses collected to know about the residence of people have been tabulated in Table 5.7. It can be observed from the statistics obtained that 18 respondents, 8.2%, resided in the villages, 92 respondents, 41.8% resided in the towns, and 110 respondents, 50% resided in cities. The statistics depict that most respondents resided in cities while a considerable segment resided in the villages.

Size of family

The size of an individual's family tells the total number of members in his family and is also, to some extent, associated with the income of an individual. It is also noteworthy that the size of an individual's family can be small or big depending upon the number of members. To know about the size of the respondents' families, the responses collected have been plotted in Table 5.7. The data plotted in the table depicts the responses obtained, which show that 12 respondents, 5.5% had 1-2 members in their

family, 148 respondents, approximately 67.3% had 2-4 members in their family, and 60 respondents, 27.3% had 3-6 members in their family. It can be inferred from the statistics that a majority of the respondents had 2-4 members in their family while a considerable segment of the respondents had prominent families having 3-6 members in their families.

Type of current residence

While this research, place of residence has been given significant consideration, the type of current residence is also considered necessary. In this section, the type of residence has been enquired to know whether the respondents have their residence or live in a rented residence. The responses collected to know about this aspect have been plotted in Table 5.7. Interestingly, it can be noticed from the table that 172 respondents, 78.2%, have their own house while 48 respondents, 21.8%, live in rented houses. The data obtained depicts that a majority of the population of the respondents live in their own house while some live-in rented houses too.

Awareness about Internet technologies

Undeniably, it can be affirmed that most people are not aware of the internet technologies existing in the world and hence cannot understand the pros and cons of using the internet. However, it is necessary to understand these technologies or have basic knowledge about them since our day-to-day jobs are connected with the internet in this present digital era. Even the education of children is now based on the internet rather than on books. To know about the awareness of internet technologies among parents, the responses gathered have been plotted in Table 5.8.

It can be observed that 159 respondents, approximately 72.3%, affirmed that they are aware of internet technologies while 61 respondents, 27.7%, denied that they were not aware of internet technologies. It is noteworthy from the statistics that a majority of the respondents are aware of internet technologies while a small segment is not aware of it.

Awareness about social networking sites

Like the lack of awareness about internet technologies, numerous respondents lack awareness about social networking sites. This lack of awareness can be due to numerous reasons, such as a shortage of smartphones and computers. It is also possible that some respondents might not have primary education about computers. To know about the awareness of people about social networking sites, the responses gathered have been

plotted in Table 5.8. It can be observed from Table 5.8 that 170 respondents, 77.3%, affirmed that they are aware of social networking sites while 50 respondents, 22.7%, are not aware of social networking sites. The statistics obtained demonstrate that there is still a significant population of respondents who are not aware of social networking sites. In contrast, a majority of the respondents are aware of it.

Table 5.8: Parents Background of Internet Technologies

Group item	**Individual item**	**Respondents**	**Percentage**
Technology awareness	Yes	159	72.3
	No	61	27.7
Social networking sites awareness	Yes	170	77.3
	No	50	22.7
E-learning tools awareness	Yes	158	71.8
	No	62	28.2
Frequency of using internet	Everyday	132	60.0
	Sometimes	71	32.3
	Not at all	8	3.6
	Cannot say	9	4.1
The device used for accessing the internet	Computer	108	49.1
	Mobile	112	50.9
Giving phones to children	Sometimes	169	76.8
	Whenever he/she asks for it	51	23.2
Monitor your kids	Yes	161	73.2
	No	59	26.8
Usage of social networking site	Yes	160	72.7
	No	60	27.3
Kid complaining about online fraud	Yes	145	65.9
	No	75	34.1

Awareness about e-learning tools and technologies

As already discussed in the previous sections, even in this present era of technology, some people are not aware of the technological changes taking place around them. It is also undeniably affirmed that technology has touched almost every part of our lives, including medical and education. The inclusion of e-learning in schools has motivated children and teachers to be familiar with the technology. However, it is also encouraging parents to be familiar with the technology. However, some parents cannot cope with the changing world and still lack awareness of the various e-learning tools and technologies. The responses collected to know about such a population of parents have been gathered and plotted in Table 5.8.

Interestingly, the responses obtained demonstrate that 158 parents (71.8%) are familiar with e-learning tools and technologies. In contrast, a lesser yet significant population, 62 parents (28.2%), denied that they are not aware of e-learning tools and technologies. It can be observed from the table that a majority of the respondents are aware of e-learning tools while a small population is not yet aware of them.

Use of internet

The responses obtained in the previous few sections exhibit that a significant population of parents is not familiar with the technological changes taking place around them, which might be due to a lack of using the internet. Also, to find out the frequency of parents towards using the internet, some responses have been collected and plotted in Table 5.8. It can be observed from the table that 132 parents (60.0%) told that they use the internet every day, 71 parents (32.3%) reported that they used the internet only sometimes, eight respondents (3.6%) told that they do not use the internet at all. Nine respondents (4.1%) said they could not say anything about how often they use the internet. It can be inferred from the statistics that a majority of the parents use the internet every day while a significant population denied that they do not use the internet frequently.

The device used for online content access

Since the markets are flooded with different types of smartphones, tablets, i-pads, the population of respondents using laptops or computers decreases. However, having craze using hi-tech devices for professional or personal use still prefers to use computers and laptops. Here it has been enquired what type of device is most preferred by the parents for accessing the internet, and the responses obtained are plotted in Table 5.8. It is noteworthy that 108 parents (49.1%) told that they access online content only through computers, while a slightly higher population, 112 respondents (50.9%) told that they access online content through mobile phones. It can be inferred from the statistics that a majority of the respondents preferred to use mobile phones due to their ease of handling them. However, a significant population preferred to use the computer due to their viewing content on a large screen.

Give your phone to the child

Undeniably, children today are far much ahead in technology than the previous generation. They are well familiar with the use of smartphones and computers. Since

they can access the devices owned by their parents, elder siblings, it is noteworthy whether parents are cautious about the quality of online content. Thus, to know whether parents, elder siblings give their phones to children or not, the responses collected have been plotted in Table 5.8. It is noteworthy that a higher percentage of the respondents, 169 parents (76.8%), said that they sometimes give their phones to children, while 51 parents (23.2%) reported that they give phones to their children whenever they ask for it. It can be inferred from the statistics that a majority of the parents gave their phones to their children only sometimes, either for the sake of fun or for searching for some educational content. In contrast, a significant population gave their phones whenever their children asked without being concerned about the purpose or need.

Monitor your kid

It has been noticed that cybercrime incidents are most commonly observed when children are not provided proper guidance or are given a free hand to do whatever they like. To avoid them, it is necessary that children be monitored and should be allowed to use internet-associated facilities only when parents know the purpose. The responses collected to know whether parents monitor their kids or not for using the internet have been plotted in the table below Table 5.8. Significantly, it can be observed from the table that 161 respondents (73.2%) said that they monitor their kids' activities and are aware of their purpose of using the internet. In comparison, 59 respondents (26.8%) said that they do not monitor their children and are unaware of their kids' purpose using the internet. It can be inferred from the statistics that most parents monitor their kids to know for what purpose they are using the internet. At the same time, a significant population denied that they do not perform any such action.

Use of social networking sites

It has been identified that a majority of the parents are addicted to using the internet and also that a significant segment is fond of being involved in socialization. In this section, an attempt has been made to know whether users access social networking sites (SNS) or not. The responses collected to know about this aspect have been plotted in Table 5.8. It can be observed from the responses obtained that those 160 respondents (72.7%) affirmed that they use SNS while 60 respondents denied that they do not use any SNS. It has been observed in the previous sections that parents are addicted to using

the internet. Hence, in this section, unsurprisingly, it can be observed that a majority of the parents use SNS while a small population has still abstained from its use.

Kid complaining about online fraud

As discussed in the previous section, the people accessing the internet can complain to the service providers. Similarly, children also experience fraud, blackmailing, and cheating complaints to their parents and elders. Some children get scared and do not discuss their thoughts or feelings with others. Hence, in this section, the responses have been collected from parents to know whether their kids' complain about online fraud or not. The responses gathered have been plotted in Table 5.8. It can be observed from the table that 145 parents (65.9%) said that their kids complain about online cheating and blackmailing, while 75 parents (34.1%) said that their kids do not make any such complaint. It can be inferred from the statistics plotted that a majority of the parents told that their children make such complaints which might be due to use of the internet for a more significant period by them. While on the other side, the other segment said that their children do not make such complaints. It might be because their children are not visiting such sites.

5.6. Descriptive Analysis for Parents

In the previous section of this chapter, a detailed discussion of parents' demographic constructs has been provided. However, in this section, a detailed description of factors allied with cybercrime has been performed. The results obtained from the responses gathered from respondents have been presented in the form of mean and standard deviation.

Cybercrime avoidance

In this section of descriptive analysis, various approaches allied with preventing the growth of cybercrime have been discussed. Here it has been identified that up to what extent parents find these approaches useful. The responses obtained for this aspect have been plotted in Table 5.9. The ability to use computers technologies and the internet effectively helps develop good interpersonal associations and encourages imagination, self-expression, and independent identity creation. Over 80% of the respondents felt that the internet and other computer technologies help develop good interpersonal associations. They have good exposure to technologies, which will also help them be

more creative and imaginative (M=4.01, SD=1.00). It was observed that 78% of the respondents felt that having more exposure to social networking and other social media sites helps improve digital social skills. They gain more awareness about what is going around them, be aware of cybercrime activities, and be cautious. (M=3.92, SD=1.07). Internet exposure has its advantages and disadvantages. 78% of the respondents felt that avoiding unwanted contact can reduce the risk of cybercrime. People who use the internet frequently will be aware of suspicious sites, and it is best to avoid them rather than become a victim of cybercrime. (M=3.91, SD=1.04).

Cybercrime can be avoided in many ways 68% of the respondents felt that reducing unwanted online habits can avoid cybercrime significantly. Avoiding phishing and malicious sites which look suspicious can help to reduce cybercrime to a significant level (M=3.48, SD=1.14). On the other hand, 46% of the respondents felt that Confining children to the home and furnishing them with media and technology will make the child's bedroom a more attractive alternative to the apparent dangers of the outside world as the child will not be aware of the dangers of cybercrime taking place. Hence, it is vital to keep track of the child's online activities to not fall prey to any online cybercrime (M=2.32, SD=1.06).

Confining children in the home and furnishing them with media and technology can invite the possibility of stranger danger; therefore, 76% of the respondents felt that children must not be confined to the four walls of the homes. They need to go out and play too(M=3.84, SD=1.01). Reducing online risk may curb online opportunities 46% of the respondents felt that if they do not use the internet and other technologies much, it may reduce the number of other opportunities as nowadays most of the opportunities are available on the internet first (M=2.39. SD=1.33) higher the standard deviation suggests more variation which signifies that there is a probability that significant 56% of the respondents do not agree with this.

There are many pornographic sites on the internet which has lots of ill effects on children. It was estimated that over 78% of the respondents felt that pornographic sites incite various kinds of violence due to the content which is available online; it instigates people towards violence, thereby increasing the crime rate (M=3.46, SD=1.14). Similarly, Pornography and other similar material would include 'hate sites' and material that appears to encourage or celebrate forms of self-harm, which might cause

much cybercrime. Approximately 72% of the respondents felt that pornography and other sites could cause a lot of hate crime due to the harmful effects of those content (M=3.67, SD=1.09).

Most parents observed that 74% of the respondents encouraged their children's early access to the Internet. By yielding their chances to explore and play online so that the children can enjoy and stay quiet, it is not a good thing to be exposed to the internet at such an early age (M=3.76, SD=1.03). Pornographic content on the internet is hazardous. It often results that the sex sites were retrieved by accident when a child, often doing homework, used a harmless word to search for information or pictures 70% of the respondents believed that children suddenly come across these contents which can harm them. It is better to ban these sites so children cannot access them, and cybercrime can be reduced (M=3.44, SD=1.26).

It was found that approximately 74% of the respondents felt that pornography and sexualized material could influence the moral values, sexual activity, and sexual attitudes of children and youth, including their attitudes toward sexual violence as children watching these can get affected adversely. Their behavior may harm them and may increase sexual violence among the youth (M=3.75, SD=1.17).

The Internet has a positive impact on their children's advancement in school and preparation for professional life. There are many advantages and disadvantages of the internet 70% of the respondents felt that the internet could have many advantages as it can help children gain more knowledge as the vast amount of information is available on the net. They can also improve their professional life by learning job-related skills online for better growth (M=3.56, SD=1.12). On the other hand, there are various drawbacks to the internet. Children and young people keep in touch with each other via instant messengers, webcams, and social network sites. 78% of the respondents felt that, unfortunately for some children, it brings negative shades because of hurtful messages and bullying because many children are innocent and not aware of the adverse effects of social media and fall prey to bullying by other people (M=3.42, SD=1.27). The government can avoid cybercrime and bullying 72% of the respondents believed that access to these sites could be restricted by having strict security measures so children cannot view these sites. It will reduce cybercrime and bullying (M=3.69, SD=1.06). Children must have aware of the dangers and risks of the internet. Hence

66% of the respondents felt that teaching them responsible behavior on the web, making them aware of the dangers they might face, and prevent the incidence of online risks can help in reducing cybercrime. It can reduce the incidents of cybercrime and bullying (M=3.30, SD=1.33). Many parents think that giving their children mobile phones and access to the internet is a sign of good socio-economic status. This thinking of parents needs to be corrected as 52% of the respondents believed that children could get access to various things and be victims of cyberbullying and crime due to no proper supervision from parents(M=2.69, SD=1.22).

It is challenging to keep track of a child's activities as parents cannot monitor daily, due to which many children fall prey to cybercrime. Therefore, 50% of the respondents felt that avoiding grooming and offender by denying the parent's trust can help avoid cyber abuse; hence, it is important for children not to deny parent's trust and misuse the internet where they ultimately fall prey to them cybercrime (M=2.56, SD=1.28). It was observed that 70% of the respondents felt that identifying which circumstances pose what kind of risk, which factors mean that risk is increased or reduced, and when risks do not result in tangible harm can avoid cyber child abuse. It is possible only through awareness among children and parents where they can identify the risks and benefits of the internet and cybercrime can be avoided. Parents should be able to identify the risks and decide about the consequences. Through which many incidents of child abuse can be avoided (M=3.50, SD=1.25).

Table 5.9: Cyber Crime Avoidance- Parents

Item	Mean	Std. Dev.
The ability to use computers technologies and the internet effectively entails good interpersonal associations and encourages imagination, self-expression, and independent identity creation	4.0136	1.00900
It is also significant in reinforcing a sense of belonging or social networking and contributes to the growth of digital social skills	3.9227	1.07628
Avoiding unwanted contact can reduce the risk of cyber solicitation and allied crime	3.9136	1.04981
Reducing unwanted online habits can avoid cybercrime significantly	3.4864	1.14469
Confining children to the home – and furnishing them with media and technology that will make the child's bedroom a more attractive alternative to the apparent dangers of the outside world	2.3227	1.06862
Confining children to the home – and furnishing them with media and technology can invite the possibility of stranger danger	3.8409	1.01007
Reducing online risk may curb online opportunities	2.3955	1.33549
Pornography contents online incite violence of various kinds	3.4636	1.14818
Pornography and other similar material would include 'hate sites', as well as material that appears to encourage or celebrate forms of self-harm	3.6727	1.09885
The majority of parents encourage their children's early access to the Internet by yielding their chances to explore and play online	3.7636	1.03304
The sex sites were retrieved by accident when a child, often in the process of doing homework, used a harmless word to search for information or pictures	3.4455	1.26842
Pornography and sexualized material can influence the moral values, sexual activity, and sexual attitudes of children and youth, including their attitudes toward sexual violence	3.7545	1.17575
The Internet has a positive impact on their children's advancement in school, as well as on preparation for professional life	3.5636	1.12284
Children and young people keep in touch with each other via instant messengers, webcams, and social network sites; unfortunately for some children, it brings negative shades because of hurtful messages and bullying.	3.4273	1.27110
Restrict access to specific web pages can avoid cyber bullying and crimes	3.6909	1.06197

Teaching them responsible behavior on the web, making them aware of the dangers they might face, and prevent the incidence of online risks can help in reducing cybercrime	3.3091	1.33957
Avoiding the perception that enabling children with internet-connected devices is a sign of socio-economic status can help to reduce cyberbullying	2.6955	1.22864
Avoiding grooming and offender by denying the parent's trust can help to avoid cyber abuse	2.5682	1.28918
Identifying which circumstances pose what kind of risk, which factors mean that risk is increased or reduced, and when risks do or do not result in tangible harm can avoid cyber child abuse	3.5045	1.25147
Parents must be able to begin educating their children at home about the risks associated online and be able to take defensive methods on the safety of their devices at home	3.6545	1.09325
Avoid children to download applications without their permission	3.4227	1.22695
Enabling web personalization data and sharing it with local administrative agencies or monitoring agencies can help to avoid both online as well as offline predators	3.5455	1.11966
Parental control software to restrict app installation or use can also be a vital solution	3.6500	1.21266
Providing parents software to monitor activities such as the use of computer programs, websites visited, chat room activity, and social network sites accessed can help to avoid kids indulging in inappropriate links	3.3364	1.32608

Parents must be able to begin educating their children at home about the risks associated online and be able to take defensive methods on the safety of their devices at home 72% of the respondents believed that parents should take responsibility and educate their children about the risks of online child exploitation and cybercrime security. They must also be taught about the ill effects of cybercrime so that children do not fall prey to any of these phishing and malicious sites, which can negatively impact them. Parents can also keep phone locks so that children do not access the internet without their knowledge and monitor their child's activities (M=3.65, SD=1.09).

The internet today has a vast number of applications available which can be downloaded easily without any permission. Some of these applications can have adult contents that children can access accidentally; therefore, 78% of the respondents felt that children must not download these applications without their permission. Hence, all applications with any adult content need to have proper security measures so

children do not access it, reducing the number of cybercrime incidents (M=3.42, SD=1.22).

The data which is available on the internet is not personalized; anyone can access it 70% of the respondents felt that the local administrative agencies must keep a check on the content that is posted on social media and the internet and should remove it immediately if they feel it has any explicit content or any insensitive remarks they can immediately block these types of contents which can help to avoid offline as online predators and children will not fall prey to them (M=3.54, SD=1.11).

There are many ways to curb online child abuse and exploitation; one of the ways can be by installing parental control software installed in phones. Approximately 72% of the respondents felt that this would help restrict app installation, which can be a vital solution for online child exploitation. The parental control software can monitor all the child's activities, which will prevent the child from accessing any unwanted adult content (M=3.65, SD=1.21). Similarly, 66% of the respondents felt that providing parents software to monitor activities such as the use of computer programs, websites visited, chat room activity, and social network sites accessed can help to avoid kids indulging in inappropriate links as these software's can help parents keep a check on their children. With the help of this software, parents can block specific websites and monitor their child's activities. The parents can also guide their children on what to browse and the risks of the internet. By following these methods, cybercrime can be avoided (M=3.33, SD=1.32).

5.7. Demographic Analysis for Technical Experts

In the previous section, the views of parents towards cybercrime and the need for measures for controlling the escalation in cybercrime have been discussed. The perspective of parents has been explored fully; however, it is of paramount significance that the perception of technical experts is also discussed. Thus, in this section, the demographic constructs of technical experts have been considered significant, and a brief discussion is made.

Gender

Gender has been a predominant factor for any research work. Gender plays a vital role in analyzing one's perspective as it is has been observed that males and females have a

different perspectives towards different things taking place around them. Hence, knowing gender plays an important role in analyzing an individual perspective towards cybercrime avoidance in this research work. It can be observed from Table 5.10 that 36 out of 50 respondents were male (72%), while 14 were female (28%). It can be inferred from the statistics that a majority were males (72%) while a significant percent (28%) were females. The statistics discussed are plotted through the graph.

Age of the respondents

The age of the respondent is an essential factor. With age comes maturity and the responsibility to answer the questions properly. In this research, the age group of the respondents has been categorized as between 20-30 years, 30-40 years, 40-50 years, and greater than 50 years. The responses collected are plotted in Table 5.10. From the given Table5.10 it can be observed that 25 out of 50 respondents (50%) were in the age group 20-30 years, 14 respondents (28%) were in the age group between 30-40 years, nine respondents approximately (18%) of the respondents were between 40-50 years, and two respondents (4%) were greater than 50 years of age. It can be inferred from the statistics shown below that a majority of the respondents (50%) were between the age group 20-30 years, while considerable populations of the respondents were between the age group 30-40 years.

Occupation of the respondents

Occupation of the respondents plays an important role in this research as it signifies the ability of the individual to satisfy his personal needs and improve one's economic conditions. In this research, the occupation of the respondents is categorized as Employed, self-employed, unemployed, student and shown in Table 5.10.

It can be observed that 40 out of 50 respondents (80%) were employed, four respondents (8%) were self-employed, and five respondents (10%) of the respondents were students, and one respondent (2%) was unemployed. From the statistics plotted below, it can be inferred that a majority of the respondents (80%) were employed, and a significant percentage of the population (8%) were self-employed and (2%) unemployed.

Table 5.10: Demography Information of Technical Experts

Group item	*Gender/Age/Occupation*	*Respondent*	*Percentage*
Gender	Male	36	72
	Female	14	28
Age	20-30 years	25	50
	30-40 years	14	28
	40-50 years	9	18
	>50 years	2	4
Occupation	employed	40	80
	self-employed	4	8.0
	student	5	10.0
	unemployed	1	2.0
Annual income	below 1,50,000	1	2.0
	1.5-2.5lac	3	6.0
	2.5-4lac	30	60.0
	4-5.5lac	15	30.0
	5.5-6	1	2.0
Place of residence	village	3	6.0
	town	6	12.0
	city	41	82.0

Annual income of the respondents

The annual income of the respondents has a significant impact on this research as the higher the income, and the technical experts can provide better ways to avoid cybercrime. It is very important to have a sufficient income to support the rising expenditures and improve the standard of living. In this research, the annual income of the respondents was classified as between 1.5-2 lacs, 2-2.5 lacs, 2.5-3 lacs, 3-3.5lacs, 4-5.5lacs, and 5.5-6 lacs. The responses collected are given in Table 5.10. From the given Table 5.10it can be observed that 1 out of 50 (2%) respondents was below 1.5 lacs, three respondents approximately (6%) were having an annual income of 1.5-2.5 lacs per annum, 30 respondents (60%) were having a reasonable income of 2.5-4lac another segment of the population approximately 15 respondents (30%) were having income between 4-5.5 lacs. Similarly, another fraction of the respondents (2%) had an annual income between 5.5 and 6 lacs per annum.

Place of residence

Place of residence is an important factor in this research because if the respondent is residing in a village or town, they might not have much access to the internet. Incidents of cybercrime will be much lesser than their city counterparts as they have easy access

to the internet and new technologies, leading to rising cybercrime incidents. In this research, the place of residence was classified as town, city, and village. From the statistics in the given Table 5.10, it can be noticed that three out of 50 respondents (6%) resided in the village, six respondents (12%) resided in towns, and a majority of the respondent, 41 (82%), resided in cities. From Table 5.10, it can be inferred that a majority of the respondents were from different cities, which suggests that most of the respondents had access to the internet and other technologies. A significant percentage were from towns and villages (12%) and (6%) respectively.

5.8. Descriptive Analysis for Technical Experts

A detailed discussion of demographic constructs of technical experts has been provided in the previous section. However, in this section, a detailed description of factors allied with cyber-crime has been performed. In this section of descriptive analysis, various approaches allied with preventing the growth of cyber-crime have been discussed. The responses obtained for this aspect have been plotted in Table 5.11.

Realizing the up-surging trends where even children intend to make their social presence over SNS, the predominant threat to be addressed is “Stranger Threat,” which is often caused due to making contact with someone you do not know. In such cases educating and counseling children for online internet use and SNS can be vital (M=4.22, SD=0.58). Undeniably, online activity monitoring of children using the internet-enabled phone and computers cannot be ignored to avoid cyberbullying, harassment, and exploitation (M=4.02, SD=0.91). It is important to identify all the risks and how the risk can be reduced and help curb online child exploitation (M=3.92, SD=0.80). Only cyber-crime is universally acknowledged in its various forms, such as the spreading of malicious viruses to disrupt the activities of other internet users. However still, moral guidelines are needed to deal with the problem. Therefore, it is important to maintain the right balance between the outdoor and indoor activities of the child and not expose the child to the internet at a young age (M=2.72, SD=1.37). Though, it cannot be the eventual solution, as indicated by a high standard deviation. Certain preventive measures can be developed using strict content monitoring and filtering techniques such as URL content search, keyword, demographic sensitive filtering. Though porn-type content is flooded over the internet, certain advanced data-sensitive

filtering approaches are needed. It can not only avoid unwanted stranger malicious contact but can also alleviate the possibility of pornographic addiction and affinity (M=4.28, SD=1.01).

Table 5.11: Cyber Crime Avoidance- Technical Experts

Item	Mean	Std. Deviation
Avoiding unwanted contact can reduce the risk of cyber solicitation and allied crime	4.2200	.58169
Reducing unwanted online habits can avoid cyber-crime significantly	4.0200	.91451
Confining children to the home – and furnishing them with media and technology that will make the child's bedroom a more attractive alternative to the apparent dangers of the outside world	2.7200	1.37083
Strict content monitoring and filtering (URL, content search, keyword, demographic sensitive filtering) approach be effective to avoid pornography and allied online children exploitation cases	4.2800	1.01096
Providing predefined or dedicated e-learning media such as mobile and computer with predefined content filtering provision and log detail auto-update can help avoid kids to incline in a negative direction	4.0000	.63888
Frequent search pattern filtering and parental control can be an effective solution	3.5400	1.11043
Content-sensitive session control and content-filtering can be an effective measure to avoid cyber children crime (online fraud/cheating/blackmailing/threat etc.)	4.0000	.63888
Monitor the log details of your kid and their socio-behavioral changes throughout internet access	3.9600	.78142
Enabling content block provision with the internet service provider can help to curb child online exploitation or harassment issues.	3.8800	.84853
Providing link-block option with browser to avoid accidentally seen pornographic contents forwarded by else can curb child online harassment tor bullying	4.0000	.83299
Providing auto information exchange for web access can help to prohibit children from coming in contact with bullying	3.7000	.78895

elements, or groomers can avoid cyber children exploitation or blackmail		
Avoiding grooming and offender by denying the parent's trust can help to avoid cyber abuse	3.3200	.91339
Exploiting demographic information such as location, age, previous search patterns, and allied user personalization variables can help to update parents as well as children to avoid unwanted (harmful) contacts	3.6800	.91339
Identifying which circumstances pose what kind of risk, which factors mean that risk is increased or reduced, and when risks do or do not result in tangible harm can avoid cyber child abuse can help to curb the online child exploitation problem	3.9200	.80407
Avoiding third-party applications from auto-download and media (phone data) access without permission can help to avoid private data loss and further defamation	4.0800	.75160
Avoiding any spreading of malicious viruses to disrupt the activities of other internet users	4.0400	.85619
Developing Groomers Identification system using advanced web personalization can help to curb online child exploitation or further offline offense (probability)	3.8800	.79898
Online identification of Online grooming, which is a private interaction between the groomer and their victims, can help to avoid cyber crime	3.6600	.82338
Applying web personalization potential threats towards online child abuse can be identified	3.6800	.79385
Enabling anti-recording or replication features when making online communication (video calling or multimedia sharing) can help avoiding online child abuse, blackmailing, and exploitation	3.9000	.86307
Exploiting spatial and temporal relationships between offenders can help identify possible offenders.`	3.6200	.80534
Identifying the commercial market and its circuit can help prohibit children's online sexual exploitation or allied events.	3.8200	.80026
Handling both commercial child exploitation as well as non-commercial exploitation can help to avoid up surge in cybercrime	3.8400	.79179
Filtering online pornography; violent video games; websites that espouse racial or ethnic hatred; commercial sites can play a vital role in avoiding online child abuse or exploitation.	4.0200	.71400

ICT can help human traffickers may also recruit new victims, including children, and market child sex tourism and hence Identifying such activities using web mining and personalization can help to eradicate such issue	3.9400	.79308
Cyber-bullies may use public websites and social media to broaden their audience and increase the impact on victims and hence detecting such events can be vital	4.1000	.78895
Filters or ‘parental controls can be installed on an individual computer or configured at the ISP level	3.8400	.93372
At a higher level, ISPs can block content originating from specific IP addresses that are found to be distributing content such as child abuse images	4.0200	.82040
Inducing the ability of or justification for ISPs to determine whether the content was illegal and the transparency of blocklists can help to avoid online children exploitation	3.8600	.83324
Using advanced techniques, including keyword and phrase searches to help screen out offensive content that has not been included on a black or exclusion list, can help to filter offensive content (to curb the issue of online child exploitation)	3.8400	.84177
Providing parents software to monitor activities such as the use of computer programs, websites visited, chat room activity, and social network sites accessed can help to avoid kids indulging in inappropriate links	3.8400	.81716
Built-in mechanisms to prevent children from bypassing or circumventing the filters, including password protection and other devices to prevent children from uninstalling the product or changing the settings	4.0200	.79514
Enabling web personalization data and sharing it with local administrative agencies or monitoring agencies can help to avoid both online as well as offline predators	3.6000	1.03016
Parental control software to restrict app installation or use can also be a vital solution	3.8000	.69985
parental control features with the capability for blocking, restricting, limiting, or allowing access to different features for younger children	3.8400	.76559
Putting legal constraints on the current state of art recommender system can help avoid further child online risk probability.	3.8000	.78246

To assist e-learning web-contents, certain parental control measures can be introduced, and log-access authorization can be applied in devices (M=4.00, SD=0.63). Frequent search patterns, being one of the most used recommender systems, can be the reason for unwanted or malicious content tagging on systems. Parents can apply this feature to understand a child's online behavior and can be used to manage access control (M=3.54, SD=1.11). Content-sensitive session control and content filtering can be effective measures to avoid online children exploitation or allied activities. Such provision can be given as mobile apps or software (M=4.00, SD=0.63). Search behavior and resulting socio-behavioral changes in children can be used to detect online harassment cases or exploitation probability (M=3.96, SD=0.78). Children tend to browse the net with a curiosity to know about new things; they can accidentally come across certain websites that link to certain pornographic content. Providing a link/user-block option in the browser (with a special provision of MAC-based device blocking) can be effective to avoid accidentally seen pornographic contents (M=4.10, SD=0.78) forwarded by others can curb child online harassment or exploitation (M=4.00, SD=0.83). Though a multi-party model, web-access information exchange can be an optimistically designed approach to avoid children coming in contact with certain malicious users or harassers (M=3.70, SD=0.78). Having proper security and integrity can help in making online activities much safer. Avoiding third-party applications from auto-download and media (phone data) access without permission can also help avoid personal data loss and further defamation (M=4.08, SD=0.75). Applying internet security features such as anti-virus, anti-malicious page detector, page content suitability detector can also be vital to reducing easy access to the objectionable content or web pages (M=4.04, SD=0.85).

Online grooming is usually a private interaction between the groomer and their victims, and is usually very secretive and hidden from other people and therefore detecting such groomers using their content patterns, communication details, location, data shared, spatial-temporal behavior, and communication (M=3.62, SD=0.80) can be taken into consideration (M=3.66, SD=0.82). Location tracking, IP-address tracking (M=3.82, SD=0.80), time, and intend assessment can also help to avoid child exploitation, though it demands dedication and honest effort, and information exchange (M=3.90, SD=0.86). Web-personalization can also be explored to enable web content, especially e-learning

materials when surfing. In addition, it can also help parents knowing the online search pattern of their child to take suitable preventive measures (M=3.68, SD=0.79). Most technical experts recommend using separate and dedicated centers to address such cases (M=3.84, SD=0.79). Blocking pornographic content can also reduce a major fraction of problems causing child exploitation (M=4.10, SD=0.78). Permitting children to use instant messaging to the known and pre-defined can reduce cyber stalking issues or harassment (M=3.86, SD=0.83). However, its success probability seems limited due to the child's reaction and affinity of parents to do so. Maintaining passwords or authorization-based content access can be vital (M=3.84, SD=0.81), though its success remained suspicious in the contemporary socio-technical arena. The technical experts also recommend monitoring the browsing activities of the child and sharing it with other parents as well as local administrative agencies with privacy-preserving can help curb child exploitation significantly (M=3.60, SD=1.03). In such cases, possible offenders can be easily tracked.

5.9. Demographic Analysis for Legal Experts

In the previous section, the views of technical experts towards cybercrime and the need for measures for controlling the escalation in cybercrime have been discussed. The perspective of technical experts has been explored fully; however, it is of paramount significance that the perception of legal experts is also discussed. Thus, in this section, the demographic constructs of legal experts have been considered significant, and a brief discussion is made.

Gender distribution of the respondents

In this research, gender plays an important role because males and females' thought process varies completely. They can have contrasting ideas and thoughts, which can make a significant impact. In this research, the gender distribution was taken as male and female, and various questions were put forward to 50 respondents. From the given Table5.12 it can be observed that 25 out of 50 (50%) respondents were male, and 25 (50%) respondents were female. From the data collected, both male and female respondents were equal in number, which signifies that the woman population is also gradually interested in activities to avoid cybercrime of children. From the statistics,

both male and female respondents show equal participation (50%) in activities to avoid cybercrime, which is extremely positive.

Table 5.12: Demography Information of Legal Experts

Group item	*Gender/Age/Occupation*	*Respondent*	*Percentage*
Gender	Male	25	50.0
	Female	25	50.0
Age	20-30years	10	20.0
	30-40years	16	32.0
	40-50years	17	34.0
	>50years	7	14.0
Occupation	employed	22	44.0
	self-employed	16	32.0
	student	6	12.0
	unemployed	6	12.0
Annual income	1.5-2.5lac	15	30.0
	2.5-4lac	8	16.0
	4-5.5lac	9	18.0
	5.5-6	9	18.0
	6 and above	2	4.0
	Below 1,50,000	7	14.0
Place of residence	Village	13	26.0
	Town	18	36.0
	City	19	38.0

Age of the respondents

The age of the respondents plays an important role in this research. People of different age groups think differently and have different opinions and thoughts. In this research, the data collected were classified into various age groups ranging from 20-30 years, 30-40 years, 40-50 years, and above 50 years of age, and shown in Table 5.12. From the given statistics, it can be observed that 10 out of 50 respondents (20%) were in the age group 20-30 years, 16 respondents (32%) were between 30-40 years, 17 respondents (34%) were 40-50 years and seven respondents (14%) were greater than 50 years. Noticeably from the statistics, the majority (34%) of the respondents were between 40-50 years and (32%) were between 30-40 years, which signifies that there is not much difference between the two age groups.

Occupation of the respondents

Occupation of the respondents plays an important role in this research as it determines one's ability to have a good standard of living. In this research occupation, the respondents were categorized as employed, self-employed, student, unemployed, and

agriculture, and depicted in Table 5.12. From the data collected, it can be observed that 22 out of 50 respondents (44%) were employed, 16 respondents (32%) were self-employed, six respondents (12%) were students, and six respondents (12%) were unemployed. From the statistics, it can be inferred that a majority of the respondents (44%) were employed and (32%) were self-employed. It signifies that most of the respondents were employed to earn a good living.

Annual Income of the respondents

The annual income of the respondents is highly important with the increasing expenditure and cost of living. Everyone looks forward to a good annual income for a secure future. In this research we categorized the annual income of the respondents into different groups such as income between 1,50,000 – 2,50,000 lacs per annum **,** 2,50,000-4,00,000, 4,00-5,50,000 lacs per annum,5,50,000- 6,00,000 and 6,00,000 and above. The respondents' income is shown in Table 5.12. From the statistics, it can be noticed that 15 out of 50 respondents (30%) have their annual income between 1.5-2.5 lakhs per annum, eight respondents (16%) were having income between 2.5-4lakhs per annum, nine respondents (18%) were in the range of 4-5.5 lakhs per annum similarly another (18%) of the respondents had annual income 5.5-6 lakhs per annum, and (4%) of the respondent's annual income was above six lakhs per annum. Seven respondents (14%) were having income below 1,50,000. It can be observed from the graphical representation that a majority of the respondents' annual income ranges from 1.5-2.5 lakhs per annum. It signifies that most of the respondents were from the middle-class section of the society.

Place of residence

Place of residence plays an important role in this research. The place of residence was categorized as village, town, and city. The population of respondents residing in towns and villages will not have much internet and technology access than those residing in cities. From Table 5.12, it can be observed that 13 out of 50 (26%) of the respondents resided in villages, 18 respondents (36%) resided in towns, and 19 respondents (38%) were from cities. From the statistics, most of the population (38%) were residing in cities, which suggests that most respondents had access to the internet and social media as in cities, the internet is available easily compared to villages and towns.

5.10. Descriptive Analysis for Legal Experts

In the previous section of this chapter, a detailed discussion of the demographic constructs of legal experts has been provided. In this section, a detailed description of factors allied with cyber-crime has been performed. Numerous methods have been considered to avoid cyber-crime and online child exploitation. Here we have identified up to which extent the legal experts can help in reducing cyber-crime. The responses obtained in the aspect have been provided in Table 5.13.

Table 5.13: Cyber Crime Avoidance Legal Experts

Item	**Mean**	**Std. Deviation**
Making strict regulation for content monitoring and filtering (URL, content search, keyword, demographic sensitive filtering) approach be effective to avoid pornography and allied online children exploitation cases	3.9800	1.03982
Providing strict and non-negotiable regulations for both ISP and phone manufacturers to ensure data exchange and unauthorized access can help curb online child exploitation, bullying, or blackmailing cases.	4.1400	.96911
Making rules for auto information exchange for web access can help to prohibit children from coming in contact with bullying elements, or groomers can avoid cyber children exploitation or blackmail	4.0600	.97750
Involving private-public partnerships and exploiting the most advanced technologies can help identify predators and make rules to observe the predators' activities to avoid many abuse cases.	4.1000	.95298
Making strict and special cells to identify the commercial market and its circuit can help prohibit children's online sexual exploitation or allied events.	4.1400	.96911
Handling both commercial child exploitation as well as non-commercial exploitation can help to avoid up surge in online child exploitation	3.3400	1.30321
Enabling web personalization data and sharing it with local administrative agencies or monitoring agencies can help to avoid both online as well as offline predators	3.9800	.93656

Education, health systems, law enforcement, and child protection workers should include internet solicitation in their areas of expertise so that they may provide the support and advice needed to counsel individuals who have experienced online solicitation.	3.6600	1.31878
Content risk, the internet is largely unregulated because governments cannot enforce laws and use the police. Hence applying multiparty synchronized activities can help swift predator identification and action to avoid any hazardous consequences.	3.9800	1.03982
Only cyber-crime is universally acknowledged in its various forms, such as spreading of malicious viruses to disrupt the activities of other internet users, but still, moral guidelines are needed to deal with the problem	3.9600	1.15987
There is the need to ban websites or similar platforms that promote such contents	4.1400	.96911
Governments should pay extra attention to is the development of policies and practices aimed at ensuring safety and protection for participants of the network, especially the youngest ones	4.1000	.95298
Putting legal constraints on the current state of art recommender system can help avoid further child online risk probability.	4.0600	1.13227
Taking strict action against child exploitation, child pornography, and such content sharing can avoid a major issue	4.1800	.89648
In most countries, laws against child sexual abuse material are based on the policy position that children should be protected from commercial sexual activities because they are too young to give informed and thus valid consent.	4.1200	.96129
Interests protected by the criminalization of child abuse images include protecting minors from abuse and the disruption of commercial markets in child abuse images, which may encourage offenders to seek to produce and supply additional images.	4.0400	1.04900
Poverty and migration, and social isolation can also have negative repercussions on patterns of commercial sexual exploitation of children	3.6600	1.31878

Practitioners need to use professional curiosity and judgment to explore what is going on with each young person	4.1000	.95298
Handling both commercial child exploitation as well as non-commercial exploitation can help to avoid up surge in cyber crime	4.1200	.96129
Making very strict punishment to the traffickers can help reducing child abuse and allied material production	4.0400	1.04900
Emphasizing the functional relations between parts and whole for promoting child online safety and developing strategies in measures related to Law, Technology and Procedure, Organizational Structures, Capacity Building, and International Cooperation.	3.9800	1.03982
Making strict rules and investigating agencies for monitoring ICT can help identify human traffickers and their activities, including children, and market child sex tourism. Identifying such activities using web-mining and personalization can help to eradicate such issues.	4.1000	.95298
The right of a child to be protected from violence, abuse, and exploitation is not a choice but rather an obligation under the international law	4.1200	.96129
Introducing strict regulations for the application developers (mobile or web) towards inappropriate access to the user's memory or activities.	4.1800	.89648
Introducing strict punishment for cyber stalking.	4.1000	.95298
Multi-agency approaches enable organizations to contribute their specific role whilst also developing shared actions to protect young people and pro-actively investigate abusers	4.1000	.95298
Safeguarding arrangements can be organized through forums such as Multi-Agency Sexual Exploitation (MASE) meetings and initiatives led by a Multi-Agency Safeguarding Hub (MASH)	4.1200	.96129
Governments are rather slow and cannot keep the legislation and procedural basis up to date due to the rapid development of technology	4.1800	.89648

There should be better and strict Internet governance policies	3.6600	1.31878
To raise the skills and capabilities of parents and children, the government should focus on: delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that Ofsted holds the system to account on the quality of delivery in this area	4.1800	.98333
Facilitating reporting of crime in an anonymous way, prevents and investigates the reporting of crimes targeting child including pornography, identity theft and various other crimes including hate communication	4.0600	1.05772
Providing tips, games and Internet safety information to help the young people, safety resources to teachers and professionals to safeguard the workplace and young people associated with them and finally advice for parents and caretakers for supporting children and youngsters for safe and worthy use of Internet	4.1400	.96911

Legal experts can help avoid cyber-crime up to a large extent by implementing strict regulations and laws. They found that 78% of the respondents felt that content monitoring and filtering techniques would be effective in avoiding pornography and allied online children exploitation cases(M=3.98, SD=1.03). 82% of the respondents felt that the legal experts could provide strict and non-negotiable regulations for both ISP and phone manufacturers to ensure data exchange and unauthorized access to help curb online child exploitation, bullying, or blackmailing cases. There were significant divergences of opinion on both the efficacy of filtering and the responsibility for filtering. (M=4.14, SD=0.96). 80% of the respondents felt that making a rule for auto information exchange for web-access can help prohibit children from contacting bullying elements or groomers to avoid cyber children exploitation or blackmailing (M=4.06, SD=0.97).

Approximately 82% of the respondents felt that if private and public companies collaborate in a partnership, this will help them to identify the attackers by using various techniques keyword search, content filtering, URL search techniques through which they can keep a check on the activities of the child and avoid cyber-crime and online child exploitation (M=4.10, SD=0.95). 82% of the respondents felt that having a strict

and special cell to identify the root cause of online child exploitation leads to avoiding the incidents of online child exploitation or allied events (M=4.14, SD=0.96). Over 66% of the respondents felt that commercial and non-commercial child exploitation must be handled separately with separate dedicated complaint cells by the legal experts for commercial and non-commercial child exploitation cases. Both the cases must not be handled together as too many cases will slow up the legal process. A higher standard deviation suggests more variation in the response (M=3.34, SD=1.30). Another method to avoid cyber-crime is to Enabling web personalization 78% of the respondents felt that monitoring the child's activities and all the browsing activities of the child can be shared with local administrative agencies or monitoring agencies to know if the child is browsing any explicit content. It will help them to avoid any online and offline predators (M=3.98, SD=0.93).

In order to avoid cyber-crime, 72% of the respondents felt that systems like education, health, law enforcement, and child protection workers should know about internet activities and online harassment cases. E-safety guidance from schools is helpful for children from under-resourced households where parents lack confidence or expertise with relation to digital media (M=3.66, SD=1.31). The government is facing problems monitoring the content on the internet because most of the published online content is not regulated as the government cannot use police and enforce laws. Therefore, 78% of the respondents felt that multiparty synchronized activities could help identify the attacker faster in avoiding hazardous consequences. Multi-agency arrangements to sexual exploitation with known linked issues are missing, trafficking, gang-association, violence against women and girls, and drugs and alcohol (M=3.98, SD=1.03). 78% of the respondents felt that many laws do not address the moral guidelines and policies to deal with harassment. Hence stricter laws should be formulated by the lawyers (M=3.96, SD=1.15). On the other hand, 82% of the respondents felt that the government should ban websites or similar platforms to reduce cyber-crime incidents as all the content will be filtered and blocked (M=4.14, SD=0.96). Towards the safety of the youngest ones, 82% of the respondents felt that the government should enforce much stricter laws with the help of legal experts and faster justice to the victims of cyber-crime (M=4.10, SD=0.95).

The legal experts recommended employing legal constraints on the currently being used cookies exploitation and recommendation systems that different firms apply to reach their target audiences (M=4.06, SD=1.13). It has also been found that strict action and penalty must be inculcated for those sharing pornographic content so that such events could not be repeated in the future (M=4.18, SD=0.89). Concerning child sexual abuse, a major fraction of legal experts affirm their common view that most of the laws are unframed against child sexual abuse as they are too young to give valid consent (M=4.12, SD=0.96). Considering online harassment and exploitation cases, experts find high chances of offenders circulating the images over different social or web pages. Hence, such acts must be dealt with strict and intolerable manner (M=4.04, SD=1.04). It has also been found that government and local agencies must consider personalized issues like lack of education, ignorance, awareness to deal with cyber-crime (M=3.66, SD=1.31).

Approximately 82% of the respondents felt that legal experts and other practitioners should understand the young child's mind as children are too young to understand sexual exploitation and give their consent as they still find it difficult to judge what is right and wrong (M=4.10, SD=0.95). From the data collection, it is clear that 82% of the respondents felt that the simultaneous handling of both commercial and non-commercial type child exploitation having complaint cell for both leads to faster reduction in cyber-crime (M=4.12, SD=0.96). From the study, 80% of the respondents felt that having strict laws and punishment for offenders against online exploitation and cyberbullying can reduce cyber-crime incidents (M=4.04, SD=1.04). Apart from having strict laws and guidelines, 78% of the respondents felt that it is important to promote online child safety and develop strategies towards developing law, technology and procedure, organizational structures, capacity building, and international Cooperation (M=3.98, SD=1.03). 82% of the respondents felt that having strict rules and investigating agencies for monitoring ICT can help identify human traffickers and their activities, including children, and market child sex tourism with internet technologies like web mining (M=4.10, SD=0.95). Every child has the right to be protected against violence, abuse, and exploitation; therefore, 82% felt that the law must be equal for everyone (M=4.12, SD=0.96). Considering mobile applications, 82% of the respondents felt that the application developers should not have unauthorized access

to the details of the users, which can be of threat to the security and confidentiality of the data (M=4.18, SD=0.89). Over 82% of the respondents felt that stalking should be made a punishable offense with help of legal experts (M=4.10, SD=0.95).82% of the respondents felt that organizing forums such as Multi-Agency Sexual Exploitation (MASE) meetings and initiatives led by a Multi-Agency Safeguarding Hub (MASH) helps in addressing all the issues related to cyber-crime and online child exploitation which must also be supported by the government (M=4.12, SD=0.96). Governments are very slow in updating 82% of the respondents felt that due to rapid development of technology, the government and the legislation could not be kept up to date due to which the procedures regarding the legislation is very slow, which results in a huge number of cases pending (M=4.18, SD=0.89). 72% of the respondents felt that the government should implement stricter policies regarding the published content. (M=3.66, SD=1.31). It is significant to create awareness among the parents and children on e-safety 82% of the respondents felt schools should include programs about e-safety in their curriculum by conducting a separate awareness program (M=4.18, SD=0.98). It is often noticed that 80% of the respondents feel that this prevents the investigation and reporting of crime, including child pornography and various forms of hate communication. It was observed that police would investigate the crime in a serious manner (M=4.06, SD=1.05). From the data collected, it was observed that 82% of the respondents felt that it is important to provide tips, games, and Internet safety information from the parents, teachers, and caretakers to help the young All these techniques will help in creating awareness about cyber rime and reduce the incidents of cyberbullying, online child exploitation, blackmailing, fraud etc. (M=4.14, SD=0.96).

5.11. Synthesis Stake Holder Analysis

This section discusses the statistical assessment of the different hypotheses defined in this study. Noticeably, to perform hypothesis testing in this study researcher applied Pearson Correlation Coefficient (P) value with a significant level of 0.05. The detailed discussion is given as follows.

Major Findings based on comprehensive data analysis

Finding 1-Impact of online Activities on Socio-educational development of Children

H_{00}: Online activities do not have a significant impact on the socio-educational development of children.

H_{10}: Online activities have significant impact on socio-educational development of children.

Table 5.14: Person Co-relation Values- Finding 1

Demographic constructs(DC)	Pearson Correlation	1	.415**	-.317**	.775**	-.265**	.177**
	Sig. (2-tailed)		.000	.000	.000	.000	.003
	N	280	280	280	280	280	280
Subject matter Information (SMI)	Pearson Correlation	.415**	1	.245**	.479**	-.034	.026
	Sig. (2-tailed)	.000		.000	.000	.572	.667
	N	280	280	280	280	280	280
Career decision and reviews(CDR)	Pearson Correlation	-.317**	.245**	1	-.129*	.425**	-.097
	Sig. (2-tailed)	.000	.000		.031	.000	.107
	N	280	280	280	280	280	280
Knowledge gaining(KG)	Pearson Correlation	.775**	.479**	-.129*	1	-.118*	.231**
	Sig. (2-tailed)	.000	.000	.031		.049	.000
	N	280	280	280	280	280	280
E learning contents(EC)	Pearson Correlation	-.265**	-.034	.425**	-.118*	1	.315**
	Sig. (2-tailed)	.000	.572	.000	.049		.000
	N	280	280	280	280	280	280
Education & personality development(EPD)	Pearson Correlation	.177**	.026	-.097	.231**	.315**	1
	Sig. (2-tailed)	.003	.667	.107	.000	.000	
	N	280	280	280	280	280	280
**. Correlation is significant at the 0.05 level (2-tailed).							

Table 5.14 illustrates the Pearson correlation values of online activities having a significant impact on the socio-education development of children. The given table

below illustrates the Pearson correlation values of online activities having a significant impact on the socio-education development of children. Various factors contributing to the socio-educational development of the children have been considered. From the given table, Pearson correlation values are greater than the significant level (p=0.05). Noticeably, since the P-value obtained for each variable is higher than the significant level (p=0.05), it affirms rejection of the null hypothesis, and hence alternate hypothesis is accepted.

Finding 2- Impact of Socio behavioral monitoring

H_{01}: Socio-behavioral monitoring cannot help avoiding online child exploitation.

H_{11}: Socio-behavioral monitoring can be helpful in avoiding online child exploitation.

Table 5.15: Person Co-relation Values- Finding 2

Apparent Dangers(AD)	Pearson Correlation	1	.001	-.487**	-.518**	.408**	.136*
	Sig. (2-tailed)		.985	.000	.000	.000	.044
	N	220	220	220	220	220	220
Stranger Danger(SD)	Pearson Correlation	.001	1	.043	-.234**	-.131	.078
	Sig. (2-tailed)	.985		.522	.000	.052	.252
	N	220	220	220	220	220	220
Restricted Access(RA)	Pearson Correlation	.487**	.043	1	.281**	-.194**	.178**
	Sig. (2-tailed)	.000	.522		.000	.004	.008
	N	220	220	220	220	220	220
Responsible Behavior(RB)	Pearson Correlation	.518**	-.234**	.281**	1	-.326**	-.256**
	Sig. (2-tailed)	.000	.000	.000		.000	.000
	N	220	220	220	220	220	220
Parental Control (PC)	Pearson Correlation	.408**	-.131	-.194**	-.326**	1	.017
	Sig. (2-tailed)	.000	.052	.004	.000		.805
	N	220	220	220	220	220	220
Activity Monitoring(AM)	Pearson Correlation	.136*	.078	.178**	-.256**	.017	1
	Sig. (2-tailed)	.044	.252	.008	.000	.805	
	N	220	220	220	220	220	220
**. Correlation is significant at the 0.05 level (2-tailed).							

Observing the overall correlation results, the major variables have the p-value more than the significant level of 0.05, which signifies rejection of the null hypothesis and

the acceptance of the alternate hypothesis. However, noticeably, there are numerous components or variables which are (strongly) negatively related to each other.

Finding 3-Impact of Log-based parental control technique and auto-information exchange measures on Cyber Crime Avoidance

H_{02}: Log-based parental control technique and auto-information exchange measures do not have significant impact on cyber-crime avoidance.

H_{12}: Log-based parental control technique and auto-information exchange measures have significant impact on cyber-crime avoidance

Table 5.16: Person Co-relation Values- Finding 3

Content Monitoring and Filtering (CMF)	Pearson Correlation	1	-.083	.000	.373**	-.127	.097	-.020	.254	-.205
	Sig. (2-tailed)		.567	1.000	.008	.381	.503	.888	.075	.154
	N	50	50	50	50	50	50	50	50	50
Search pattern Filtering (SPF)	Pearson Correlation	-.083	1	.201	.167	-.125	.552**	-.091	.037	-.112
	Sig. (2-tailed)	.567		.161	.248	.388	.000	.530	.800	.437
	N	50	50	50	50	50	50	50	50	50
Content-sensitive session control (CSSC)	Pearson Correlation	.000	.201	1	.409**	-.038	-.192	-.040	-.183	.542**
	Sig. (2-tailed)	1.000	.161		.003	.795	.182	.780	.204	.000
	N	50	50	50	50	50	50	50	50	50
Monitoring log details(MLD)	Pearson Correlation	.373**	.167	.409**	1	.147	.408**	-.185	.321*	.637**
	Sig. (2-tailed)	.008	.248	.003		.310	.003	.197	.023	.000
	N	50	50	50	50	50	50	50	50	50
Content block provision with internet service provider (BISP)	Pearson Correlation	-.127	-.125	-.038	.147	1	.318*	.329*	.165	.064
	Sig. (2-tailed)	.381	.388	.795	.310		.025	.020	.252	.658
	N	50	50	50	50	50	50	50	50	50
Link Block option(LBO)	Pearson Correlation	.097	.552**	-.192	.408**	.318*	1	.124	.350*	-.128
	Sig. (2-tailed)	.503	.000	.182	.003	.025		.390	.013	.376
	N	50	50	50	50	50	50	50	50	50
Auto Information Exchange(AIE)	Pearson Correlation	-.020	-.091	-.040	-.185	-.329*	.124	1	-.185	-.250
	Sig. (2-tailed)	.888	.530	.780	.197	.020	.390		.199	.080
	N	50	50	50	50	50	50	50	50	50

Observing the above-stated results, it can be found that the p-value obtained for the variables is higher than the significant level (0.09). Therefore the null hypothesis is rejected, and the alternate hypothesis is accepted.

Finding 4 –Implementation of strict regulation for online content filtering and monitoring

H_{03}: Forming and implementing strict regulation for online content filtering and monitoring cannot effectively alleviate online child exploitation.

H_{13}: Forming and implementing strict regulations for online content filtering and monitoring can be effective for alleviating online child exploitation.

Table 5.17: Person Co-relation Values- Finding 4

Content Monitoring and Filtering(CMF)		Pearson Correlation	1	.833**	.965**	.796**	.441**	.799**
		Sig. (2-tailed)		.000	.000	.000	.001	.000
		N	50	50	50	50	50	50
Regulation for ISP and phone manufacturers(RIM)		Pearson Correlation	.833**	1	.831**	.790**	.453**	.748**
		Sig. (2-tailed)	.000		.000	.000	.001	.000
		N	50	50	50	50	50	50
Auto Information Exchange(AIE)		Pearson Correlation	.965**	.831**	1	.804**	.459**	.766**
		Sig. (2-tailed)	.000	.000		.000	.001	.000
		N	50	50	50	50	50	50
Local Administrative agencies(LAA)		Pearson Correlation	.796**	.790**	.804**	1	.523**	.784**
		Sig. (2-tailed)	.000	.000	.000		.000	.000
		N	50	50	50	50	50	50
Involvement of Law Enforcement agencies and Child protection Agencies (LECP)		Pearson Correlation	.441**	.453**	.459**	.523**	1	.542**
		Sig. (2-tailed)	.001	.001	.001	.000		.000
		N	50	50	50	50	50	50
Anonymous reporting(AR)		Pearson Correlation	.799**	.748**	.766**	.784**	.542**	1
		Sig. (2-tailed)	.000	.000	.000	.000	.000	
		N	50	50	50	50	50	50

Parental Control(PC)	Pearson Correlation	.254	.037	-.183	.321*	.165	-.350*	-.185	1	.282*
	Sig. (2-tailed)	.075	.800	.204	.023	.252	.013	.199		.047
	N	50	50	50	50	50	50	50	50	50
Blocking restricting and Limiting(BRL)	Pearson Correlation	-.205	-.112	-.542**	.637**	.064	-.128	-.250	.282*	1
	Sig. (2-tailed)	.154	.437	.000	.000	.658	.376	.080	.047	
	N	50	50	50	50	50	50	50	50	50
**. Correlation is significant at the 0.05 level (2-tailed).										

Observing overall results, the P-value for the variables under study is higher than the significant level of 0.05, which signifies rejection of the null hypothesis and the acceptance of the alternate hypothesis.

Table 5.18: Person Co-relation Values- Finding 5

Ban websites (BW)	Pearson Correlation	1	.692**	.736**	.675**	.726**	.726**	.737**	.833**	.692**
	Sig. (2-tailed)		.000	.000	.000	.000	.000	.000	.000	.000
	N	50	50	50	50	50	50	50	50	50
Government policies and procedures(GPP)	Pearson Correlation	.692**	1	.751**	.838**	.722**	.722**	.792**	.702**	1.000**
	Sig. (2-tailed)	.000		.000	.000	.000	.000	.000	.000	.000
	N	50	50	50	50	50	50	50	50	50
Legal constraints (LC).	Pearson Correlation	.736**	.751**	1	.733**	.799**	.799**	.857**	.798**	.751**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000	.000	.000
	N	50	50	50	50	50	50	50	50	50
Legal Actions	Pearson Correlation	.675**	.838**	.733**	1	.661**	.661**	.708**	.683**	.838**
	Sig. (2-tailed)	.000	.000	.000		.000	.000	.000	.000	.000
	N	50	50	50	50	50	50	50	50	50
Adoption of international law(AIL)	Pearson Correlation	.726**	.722**	.799**	.661**	1	1.000**	.784**	.819**	.722**
	Sig. (2-tailed)	.000	.000	.000	.000		.000	.000	.000	.000
	N	50	50	50	50	50	50	50	50	50
Commercial and non-commercial exploitation (CNCE)	Pearson Correlation	.726**	.722**	.799**	.661**	1.000**	1	.784**	.819**	.722**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000	.000	.000
	N	50	50	50	50	50	50	50	50	50

Punishment to the traffickers (PT)	Pearson Correlation	.737**	.792**	.857**	.708**	.784**	.784**	1	.843**	.792**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000		.000	.000
	N	50	50	50	50	50	50	50	50	50
Law, Technology and Procedures (LTP)	Pearson Correlation	.833**	.702**	.798**	.683**	.819**	.819**	.843**	1	.702**
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000		.000
	N	50	50	50	50	50	50	50	50	50
Use of Web mining (UWM)	Pearson Correlation	.692**	1.000**	.751**	.838**	.722**	.722**	.792**	.702**	1
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	
	N	50	50	50	50	50	50	50	50	50
**. Correlation is significant at the 0.01 level (2-tailed).										

Finding 5-Effectiveness of measures taken for reducing online child exploitation

H_{04}: Measures taken for reducing the impact of online child exploitation seem to be effective

H_{14}: Measures taken for reducing the impact of online child exploitation do not seem to be effective.

The statistics from Table 5.18, reveal that the p-values obtained for the different measures proposed are higher than the significant level. Therefore, the null hypothesis is rejected, while the alternate hypothesis gets accepted.

Finding 6-Impact of inter/intra socio-administrative platform with online activity and content monitoring

Ho: Developing inter/intra socio-administrative platform with online activity and content monitoring access cannot help avoiding online child exploitation.

Ha: Developing inter/intra socio-administrative platform with online activity and content monitoring access help avoiding online child exploitation.

To assess this hypothesis, primarily the responses and suggestions from the legal experts have been considered. The results from Table 5.19 signifies that the Pearson correlation coefficients of the different variables considered are higher than the significant level of 0.05. Therefore, the null hypothesis is rejected, and the alternate hypothesis is accepted.

Table 5.19: Person Co-relation Values- Finding 6

Involvement of Law Enforcement agencies and Child protection Agencies (LECP)	Pearson Correlation	1	.434**	.564**	.381**	1.000**	.489**	.453**
	Sig. (2-tailed)		.002	.000	.006	.000	.000	.001
	N	50	50	50	50	50	50	50
Multi Agency Approaches(MAC)	Pearson Correlation	.434**	1	.722**	.838**	.434**	.721**	.692**
	Sig. (2-tailed)	.002		.000	.000	.002	.000	.000
	N	50	50	50	50	50	50	50
Multi Agency approach(MAA)	Pearson Correlation	.564**	.722**	1	.661**	.564**	.732**	.726**
	Sig. (2-tailed)	.000	.000		.000	.000	.000	.000
	N	50	50	50	50	50	50	50
Slowness in government policy implementation(SGPI)	Pearson Correlation	.381**	.838**	.661**	1	.381**	.634**	.675**
	Sig. (2-tailed)	.006	.000	.000		.006	.000	.000
	N	50	50	50	50	50	50	50
Strict Internet governance (SIG)	Pearson Correlation	1.000**	.434**	.564**	.381**	1	.489**	.453**
	Sig. (2-tailed)	.000	.002	.000	.006		.000	.001
	N	50	50	50	50	50	50	50
E-Safety curriculum(ESC)	Pearson Correlation	.489**	.721**	.732**	.634**	.489**	1	.894**
	Sig. (2-tailed)	.000	.000	.000	.000	.000		.000
	N	50	50	50	50	50	50	50
Information Security Awareness(ISA)	Pearson Correlation	.453**	.692**	.726**	.675**	.453**	.894**	1
	Sig. (2-tailed)	.001	.000	.000	.000	.001	.000	
	N	50	50	50	50	50	50	50
	** Correlation is significant at the 0.05 level (2-tailed).							

5.12. Predictive Analysis and Testing Models for Child Online Safety

Background

In this digitized era, the Internet is an essential part of life and its size is increasing with more household connections. The evolution of computers and the popularity of the Internet are allowing fast communication between people. World Wide Web, Peer Peer Networks, Emails, instant messaging applications, and Social networking sites play a major role in information exchange (Chou, 2019; Thanuskodi, 2019). Safety is a major concern of the children who use Internet since it is a medium to access different types of information which could have positive and negative impacts on the children. Child online safety is a state of being protected from online problematic content and

environment. Online Child Exploitation has been a concern across the globe. Children are more victimized from exploitation than an older person (Kristensen, 2003). Online child exploitation or allied risks comes into the picture only when considering internet technologies as the use pattern. Though Internet technologies have contributed to improving the social, scientific, or economic arena, its adverse effects cannot be neglected. Understanding Internet technologies, applications, and allied vulnerable (virtual) worlds can be of paramount significance.

Internet is an important channel that helps children build their creativity, self-expression, and knowledge competency level. The available benefits of the Internet made its usage prevalent by the people and corporations for almost every activity (Livingstone and Haddon, 2009). The increasing bandwidth of the Internet is adding more users to the online world. Internet bears a wide range of risks and threats which are susceptible to children. Due to their lack of digital literacy, there exist potential risks where children could be victims of online abuses such as sexual harassment and cyber mistreat and other crimes that make children vulnerable. Acknowledging the dangers and hazards to children on the Internet depends on the blend of approaches that include self and co-regulatory, technical, legislative, educational awareness, positive content provision, and ensuring child safety zones. Every country has its own sets of policies to act against crimes related to child online safety. Different policy measures co-exist, which address these risks and initiatives from different stakeholders, creating complex policies at the national level and heterogeneous policies across different countries.

The Internet has become an integral part of the life of children for their education and social development (Singh, 2018; UNICEF, 2016). Children can access the internet easily with the help of mobile phones, laptops, tablets, desktops, and several other electronic gadgets (UNICEF, 2017). With the digital India drive and other strategic activities initiated by the Indian government alongside the enthusiasm of multinational organizations in outfitting the capability of the Indian market, are cultivating the extension of information and communication technologies (ICT) at a pace and scale never seen before (UNICEF, 2017).

In recent years, the Internet has allowed people to communicate to different parts of the world as well as provided a door to a wealth of information. Even though the Internet is considered a great tool for learning and access knowledge, the same tool exposes

children to online threats and risks. These threats and risks impact the young minds of children negatively and compromise their safety and well-being. The risks turned out to be serious, especially in developing countries. With limited resources controlling online threats such as abuse, cyberbullying, hate content, and stalking is difficult (Dombrowski et al., 2007; Singh, 2018). The Internet opens a path to various information for children but carries dangers and risks such as inappropriate content, harmful conversations, and exposure to unwanted information. Moreover, children share their personal information not being aware of the long-term privacy consequences (Whittle et al., 2007).

With these benefits and consequences of the Internet, this section tries to identify different factors associated with online child safety and confirms some of the factors influencing online child safety. The current study involves testing two different research models using the responses collected from parents and technical experts separately.

Theoretical Framework and Research Model

Increased growth of ICTs, high-speed connectivity, and wider network coverage made online activities easier and often harmful across the globe. In this digital era, strong Internet governance practices are required to protect children's rights. The Internet governance organizations can incorporate multiple stakeholders such as children, parents, teachers, Internet service providers, law enforcement agencies, and governments for their better performance. As children's online safety is a global issue, several countries have taken steps to act on it by introducing online child safety and protection-related acts and various awareness programs (Livingstone and Smith, 2014; Isaac et al., 2004; ITU, 2015; UNICEF, 2012). In this regard, the guidelines are prepared for children, parents, caretakers, policymakers, and industry by international research organizations (O'Connell 2003; ITU, 2015). The children's online safety issues may be addressed within the categories such as governance, technology, and social.

Child online safety is a state of being free from online threats like bullying, abuse, stalking, hatred, and age-inappropriate content. In this digitized era, attaining online child safety is challenging and demands a collective effort from the government, technical experts, parents, and legal advisors. In the following subsections, the literature review is done on parents, and technical experts initiated online child safety.

Parents initiated child online safety

Digital Awareness: Awareness programs (NIST, 1998) are identified as the mechanism to build a secure positive environment by alerting users on the consequences of Internet use. Safety awareness can be made through traditional media, websites, specialized awareness content from experts, and Internet service providers. To protect young Internet users, emphasis on policies is needed to raise awareness and back appropriate measures (Livingstone et al., 2012; Opstad, 2019; Weston and Mythen, 2019).

H_{P1}: Digital awareness is a predictor of parents-initiated child online safety.

Establishing wanted contact: Avoiding unwanted contact can reduce the risk of cyber solicitation and allied crime (Madigan et al., 2018). Before establishing contact with others online, it is essential to understand their background.

H_{P2}: Establishing wanted contact is a predictor of parents-initiated child online safety.

Limited online convenience: Social networking sites enable users to share their updates such as the status, content of cognition, and any specific behavior or action to friends (Jones et al., 2008; Valenzuela et al., 2009). Self-disclosure of personal information and status updates may be problematic because of the risks like identity theft, cyber-stalking, and cyberbullying. Users are more concerned about privacy, but self-disclosure is prevalent (Jones et al., 2008). The online presence can be made with the availability of technology and usage convenience (Zabatiero et Al., 2018). With limited online convenience, the online risks can be reduced.

H_{P3}: Limited online convenience is a predictor of parents-initiated child online safety.

Online benefit: Children are spending more time with the Internet and engaged in several online activities. The various concerns in this regard are cyberbullying, inappropriate content availability, addiction to the Internet, and privacy issues (Livingstone et al., 2011). As the Internet is more personal and portable, it is hard for parents to monitor children's online activities (Shin, 2015). Since the inception of the Internet, Internet addiction is identified as one of some of the most preoccupations (Burnay et al., 2015). More online presence may attract both benefits and risks (Livingstone et al., 2018).

H_{P4}: Online benefit is a predictor of parents-initiated child online safety.

Restricting resources: The proliferation of the Internet has significantly contributed to the increased availability of pornographic or sexual content and changes in

consumption of sexually explicit content by children (Owens et al., 2012). It has enhanced the probability of children accidentally accessing such content on the web. Restricting access to certain content and resources may reduce online risks (Narayanan et al., 2018).

H_{P5}: Restricting resource is a predictor of parents-initiated child online safety.

Educating on online risks: Online safety education is essential to reduce risks based on their usage pattern (Edwards et al., 2018). The efforts on widely accepted preventive measures, awareness programs, and education are made by civil societies, industries, government initiatives, and motivated individuals focusing on online etiquette for children. The existing awareness programs for children are less appropriate to a system (UNICEF, 2016). System-wide awareness programs need to be implemented by accommodating the high school and higher secondary curriculum. To provide training and workshops on online security, MEITY, a unit of the ministry of communications and information technology in India, has initiated a project on "information security education and awareness" for 2015-2020 (ISEA, 2014). A certification program in online security is also conducted for interested children by the center to develop advanced computing under this project.

H_{P6}: Educating on online risks is a predictor of parents-initiated child online safety.

Empowering authorities: A national framework is a novel approach assigning responsibility to the workforce to keep children safe. The framework establishes competencies and standards for people having direct/indirect contact with children to ensure that they deliver a systematic and consistent standard of help to children and youngsters (Hasebrink et al., 2008). A well-defined governance system for online grievance redressing (Rana et al., 2013) with a mechanism to register online, investigate and respond within a given time frame is developed. Empowering parents and concerned authorities may reduce online risks (Deb, 2018; Nawaila et al., 2018).

H_{P7}: Empowering authority is a predictor of parents-initiated child online safety.

Parental control: Victimization through the Internet is termed cyberbullying and defined as "willful and repeated harm inflicted through the medium of electronic text" (Patchin and Hinduja, 2006). Cyberbullying is an encapsulation of all forms of harm or harassment that commonly occur with the Internet, computers, and mobiles, such as sending threatening, harassing, and harmful mails or messages, posting derogative

comments, intimidating online, ignoring, disrespecting, spreading rumors, stalking and physical threatening (Hinduja and Patchin, 2007). Therefore, identification of virtual harm may reduce the possibility of victimization. Video sharing sites are associated with age-inappropriate content such as violent and pornographic content (Livingstone et al., 2013). Though the parents support their children's Internet usage, setting limits on use, content types, and time is a difficult task. Several tools are available to parents to limit the exposure of their children to age in-appropriate content (Hashish et al., 2014). The parents can control their children's online activities to reduce online risks (McNally et al., 2018; Soh et al., 2018).

H_{P8}: Parental control is a predictor of parents-initiated child online safety.

Technical experts initiated child online safety

Establishing wanted contact: Avoiding unwanted contact can reduce the risk of cyber solicitation and allied crime (Madigan et al., 2018). Before establishing contact with others online, it is essential to understand their background.

H_{T1}: Establishing wanted contact is a predictor of technical experts initiated child online safety.

Content filtering: Predators provoke children to participate in online sexual activities and broach the process through discussions on sexual nature by sending pornographic content based on children's interest using chat rooms (Normand and Sallafranque-St-Louis, 2016). Websites or applications with chatting blogs have been identified as sites with greater prevalence (YISS, 2011). Using a content filtering strategy, online risks can be reduced (Singh et al., 2018; Szafranski et al., 2018).

H_{T2}: Content filtering is a predictor of technical experts initiated online child safety.

Blocking at different levels: The mobile applications can be blocked at different levels for the safety of children (McNally et al., 2018). Similarly, online content can be monitored and blocked at different levels over the Internet (Gosh et al., 2018; DeMarco et al., 2018).

H_{T3}: Blocking at different levels is a predictor of technical experts initiated child online safety.

Education on online behavior: Young Internet users should identify online social networking fake accounts, sexual content, and connection requests from multiple accounts of the same person (Boshmaf et al., 2011). Knowledge on the activity that

children are performing online is important (Tsirtsis et al., 2016). Users accept friend requests to connect by unknown when there exist mutual friends (Boshmaf et al., 2011). Identifying strangers in the social networking profile and removing them from the friend list is essential to reduce online risks. Password sharing among family members is often a common practice (Zhang-Kennedy et al., 2016). As 33 percent of users share their passwords with friends, the possibility of compromising online safety increases (Kaye, 2011; Lenhart et al., 2011). Being cautious during sharing of passwords to friends and relatives is essential to reduce risks.

H_{T4}: Education on online behavior is a predictor of technical experts initiated child online safety.

Identification systems: Parents and teachers may supervise children's activities at home and school. Often, the limited knowledge of parents to monitor children's activities online may lead to miss experiences of the victim and checking of predator actions (Hinduja and Patchin, 2014a). Identifying illegal content sources is important to control online child risks (DeMarco et al., 2018; Klika et al., 2019).

H_{T5}: Identification systems are a predictor of technical experts initiated online child safety.

ISP-level effort: At a higher level, ISPs can block content originating from specific IP addresses that are found to be distributing content, such as child abuse images (Brennan et al., 2019). The blocking at ISP is a prevalent concept to mitigate risks (Romero Moreno et al., 2019).

H_{T6}: ISP level effort is a predictor of technical experts initiated online child safety.

Parental control: Though the parents support their children's Internet usage, setting limits on use, content types, and time is a difficult task. Several tools are available to parents to limit the exposure of their children to age in-appropriate content (Hashish et al., 2014). The parents can control their children's online activities to reduce online risks (McNally et al., 2018; Soh et al., 2018).

H_{T7}: Parental control is a predictor of technical experts-initiated child online safety

Research Model

Different variables related to online child safety are identified from a literature review. The research model for parents-initiated child online safety is shown in Figure 5.1. Digital awareness, establishing wanted contact, limited online convenience, online

benefits, restricting resources, educating on online risks, empowering authorities, and parental control are the different independent variables in the parent-initiated child online safety.

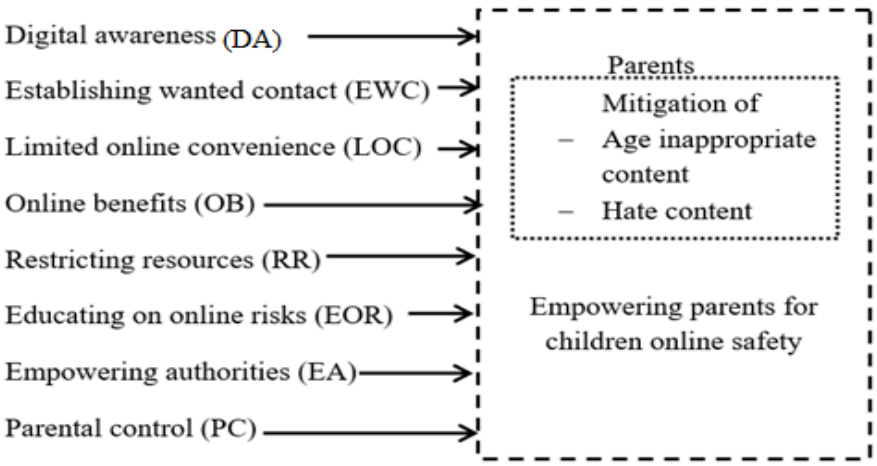

Figure 5.1: Research Model for Parent Initiated Child Online Safety

Similarly, a research model for technical experts initiated online child safety is shown in Figure 5.2. The different independent variables in technical experts initiated online child safety are establishing wanted contact, content filtering, blocking at different levels, education on online behavior, identification systems, ISP-level efforts, and parental control.

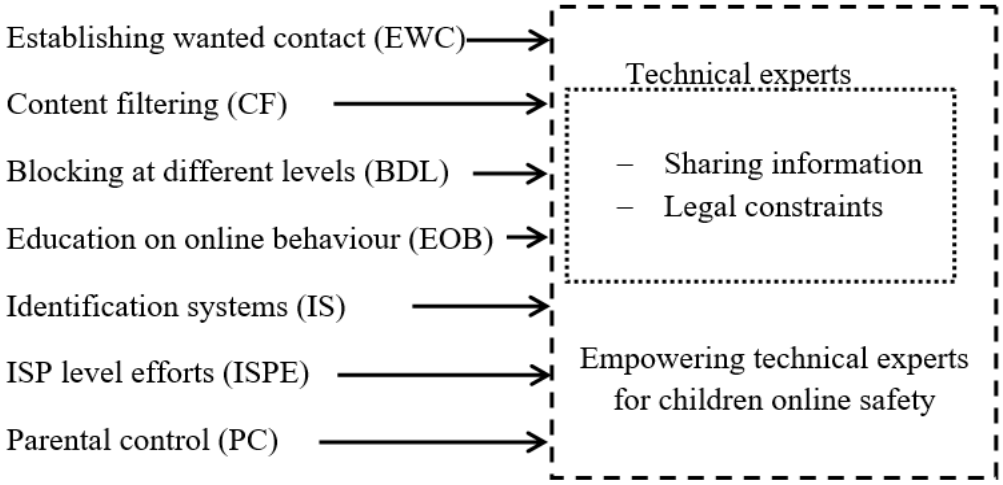

Figure 5.2: Research Model for Technical Experts Initiated Child Online Safety

Methodology

The study uses a quantitative approach to determine the predictors of online children's safety. The data is collected through online and offline modes by preparing a questionnaire and requesting the different stakeholders to fill it. The prepared questionnaire is shared through Google forms. To collect responses from the stakeholders described above, a convenient cum random sampling approach has been considered. The different stakeholders have been requested through online media such as Skype, Whatsapp, Video calls, and in-person to assess respective concerns toward escalating cybercrime, online child exploitation, leaking of personal information, and allied issues.

Two different structured questionnaires have been constructed and administered to a sample of parents and technical experts belonging to different age groups. The questionnaires are designed to retrieve meaningful information from the respondents of their respective views and perceptions of online child exploitation and various mechanisms and parental control techniques to prevent online child abuse. Both demographic and descriptive attributes related questionnaires were prepared that exploited perceptions and suggestions of the different stakeholders.

The overall questions were prepared as close-ended questions where demographic questions were framed as Yes, No, and multiple-choice type questions. The major descriptive questions were prepared using a five-point Likert scale with multiple choices (options). In other words, to exploit more significant and generalizable outcomes, questionnaires were structured along a five-point Likert's scale encompassing labels as strongly agree (5), agree (4), neutral (3), disagree (2), and strongly disagree (1). After collecting the data, both online and offline data are integrated to construct a dataset for research. The combined dataset is processed and analyzed with the help of SPSS software. The outcome of the regression algorithm is interpreted, and influencers of child online safety are identified.

Results and Discussion

The results obtained from two different models, such as parents initiated and technical experts initiated on online children safety, are represented in the following subsections.

Parent initiated online children safety

The result of his correlation will also serve as a mechanism for identifying multicollinearity among the predictors. The Pearson's correlation between the different predictors of parent-initiated online children safety along with the significant levels is shown in Table 5.20. The correlation between the APC dependent variable and RR predictor is 0.59, a larger positive correlation than the other pairwise predictors. As all the pairwise correlation values are below 0.9, there is no multicollinearity between the predictors (Field, 2009).

The result of regression analysis for parent-initiated online children safety is shown in Table 5.20. R^2 is a measure to know the variability resulting independent variables from the predictors. The model, which is designed to predict parent-initiated online children's safety, results in 0.50 as R^2 value. The effect size of the predictors on the outcome variable is more.

Table 5.20: Correlation among different Variables for Parent Initiated Model

	COS	DA	EWC	LOC	OB	RR	EOR	EA	PC
COS	1.00								
DA	0.30**	1.00							
EWC	0.46***	0.24*	1.00						
LOC	0.33**	0.23*	0.27*	1.00					
OB	0.26*	0.30**	0.34**	0.37***	1.00				
RR	0.59***	0.27*	0.51***	0.17	0.43***	1.00			
EOR	0.46***	0.24*	0.41***	0.32**	0.43***	0.56***	1.00		
EA	0.36**	0.17	0.38***	0.23*	0.34**	0.41***	0.30**	1.00	
PC	0.58***	0.09	0.52***	0.27*	0.21*	0.58***	0.45***	0.44***	1.00

**p < 0.05; **p< 0.01; ***p<0.001; COS: Child online safety; DA: Digital awareness; EWC: Establishing wanted contact; LOC: Limited online convenience; OB: Online behavior; RR: Restricting resources; EOR: Educating on online risks; EA: Empowering authorities; PC: parental control.*

The result of regression analysis for parent-initiated online children safety is shown in Table 5.20. R^2 is a measure to know the variability resulting in the dependent variable from independent variables. The model is designed for predicting the parent-initiated online children safety results 0.50 as R^2 value. The effect size of the influencers on the outcome variable is more. The F-Ratio for this model is 8.25 at a highly significant level ($p<0.001$). The F-Ratio represents the prediction ability of the model. The effect size R^2 and F represent the model's overall performance, i.e., the combined performance of all the influencers. The collinearity among variables can be checked with the variance inflation factor (VIF). As the VIF value of all measuring variables is less than

3, there is no collinearity. By referring to β values, the performance of individual predictor parameters can be measured.

From Table 5.21, a path from digital awareness to parent-initiated child online safety is not significant as its P-value is greater than 0.05. Therefore, hypothesis H_{p1} is rejected. Similarly, paths from establishing wanted contact, limited online convenience, online benefits, educating on online risks, and empowering authorities to parent-initiated child online safety are not significant as their P values are greater than 0.05. Therefore, the hypotheses H_{p2}, H_{p3}, H_{p4}, $H_{p6,}$ and H_{p7} are not accepted.

Table 5.21: Regression Analysis Results-Parent Initiated Model

Dept. Variable	R^2	F	Ind. Variable	Beta	T	VIF
Parent	0.50	8.25	Digital awareness (DA)	0.15	1.56	1.18
			Establishing wanted contact (EWC)	0.07	0.62	1.63
			Limited online convenience (LOC)	0.15	1.51	1.30
			Online benefits (OB)	-0.10	-0.93	1.55
			Restricting resources (RR)	0.31	2.45*	2.14
			Educating on online risks (EOR)	0.08	0.74	1.67
			Empowering authorities(EA)	0.04	0.34	1.38
			Parental control (PC)	0.28	2.33*	1.94

The F-Ratio for this model is 8.25 at a highly significant level ($p<0.001$). The F-Ratio represents the prediction ability of the model. The effect size R^2 and F represent the model's overall performance, i.e., the combined performance of all the predictors. The collinearity among variables can be checked with the variance inflation factor (VIF). As the VIF value of all measuring variables is less than 3, there is no collinearity. By referring to β values, the performance of individual predictor parameters can be measured.

From Table 5.21, a path from digital awareness to parent-initiated child online safety is not significant as its P-value is greater than 0.05. Therefore, the hypothesis H_{P1} is rejected. Similarly, paths from establishing known contacts, limited online convenience, online benefits, educating on online risks, and empowering authorities to parent-initiated child online safety are not significant as their P values are greater than

0.05. Therefore, the hypotheses H_{P2}, H_{P3}, H_{P4}, H_{P6} and H_{P7} are not accepted. The path from restricting resources to parent-initiated child online safety is significant as its P-value is smaller the 0.05. This significance level made to accept the hypothesis H_{P5}. Hence, restricting resources is a predictor of parent-initiated child online safety. Similarly, the path from parental control to parent-initiated child online safety is also significant as its P-value is smaller than 0.05. Hence, parental control is a predictor of parent-initiated child online safety. Therefore, the hypothesis H_{P8} is also accepted.

Technical experts initiated online children safety

The Pearson's correlation between the different parent-initiated online children's safety and the significant levels is shown in Table 5.22. The correlation between the identification systems and ISP level efforts is 0.65 and more than the other correlations. The regression analysis for technical experts initiated online children safety is shown in Table 5.23. As R^2 is a measure to know variability, the model provides 0.63 as R^2 value and results in a large effect size of the influencers on the outcome variable. F-Ratio with the value 5.36 represents the model's prediction ability at a highly significant level ($p<0.001$). There is no collinearity among variables as the VIF value of all measuring variables is less than 3.

The Pearson's correlation between the different predictors of technical experts initiated online children safety, and the significant levels are shown in Table 5.22.

Table 5.22: Correlation among different Variables for Parent Initiated Model

	COS	EWC	CF	BDL	EOB	IS	ISPE	PC
COS	1.00							
EWC	0.33*	1.00						
CF	0.03	0.40*	1.00					
BDL	-0.19	0.31*	0.50**	1.00				
EOB	0.20	0.38*	0.23	0.38*	1.00			
IS	0.32*	0.47**	0.31*	0.57**	0.38*	1.00		
ISPE	0.16	0.50**	0.16	0.49**	0.45**	0.65***	1.00	
PC	0.59**	0.35*	0.38*	0.30	0.23	0.51**	0.43**	1.00

The regression analysis for technical experts initiated online children safety is shown in Table 5.23. As R^2 is a measure to know variability, the model provides 0.63 as R^2 value and results in a large effect size of the predictors on the outcome variable. F-Ratio with the value 5.36 represents the model's prediction ability at a highly significant level ($p<0.001$). There is no collinearity among variables as the VIF value of all measuring variables is less than 3.

Table 5.23: Regression Analysis Results-Technical Experts Initiated Model

Dept. Variable	R^2	F	Ind. Variable	Beta	T	VIF
Technical Experts	0.63	5.36	Establishing wanted contact (EWC)	0.23	1.37	1.67
			Content filtering (CF)	-0.15	-0.86	1.78
			Blocking at different levels (BDL)	-0.50	-2.72*	2.04
			Education on online behaviour (EOB)	0.19	1.23	1.36
			Identification systems (IS)	0.30	1.54	2.29
			ISP level efforts (ISPE)	-0.23	-1.15	2.29
			Parental control (PC)	0.62	3.84**	1.55

A path from establishing known contacts to technical experts-initiated child online safety has a P-value of more than 0.05 and is not significant. Therefore, hypothesis H_{T1} is rejected. Similarly, paths from content filtering, education on online behaviour, identification systems, and ISP level efforts to technical experts-initiated child online safety are not significant as their P values are more than 0.05. Therefore, the hypotheses H_{T2}, H_{T4}, $H_{T5,}$ and H_{T6} are not accepted.

The path from blocking at different levels to technical experts-initiated child online safety is significant as its P-value is less than 0.05. Hence, the hypothesis H_{T3} is accepted and interpreted as blocking at different levels is a predictor of technical experts-initiated child online safety. Similarly, the path from parental control to technical experts-initiated child online safety is more significant as its P-value is lesser than 0.01. Therefore, the hypothesis H_{T7} is also accepted. Hence, parental control is also a predictor of technical experts-initiated child online safety. The set of determinants of contributors to online child safety are shown in Figure 5.3.

The analysis shows that restricting resources influences online child safety. It indicates that facilitating children with limited resources such as Internet connection, Internet

speed, and connecting devices for online activities results in less online presence, resulting in reduced exposure to online threats. Restricting websites is also a part of restricted resources.

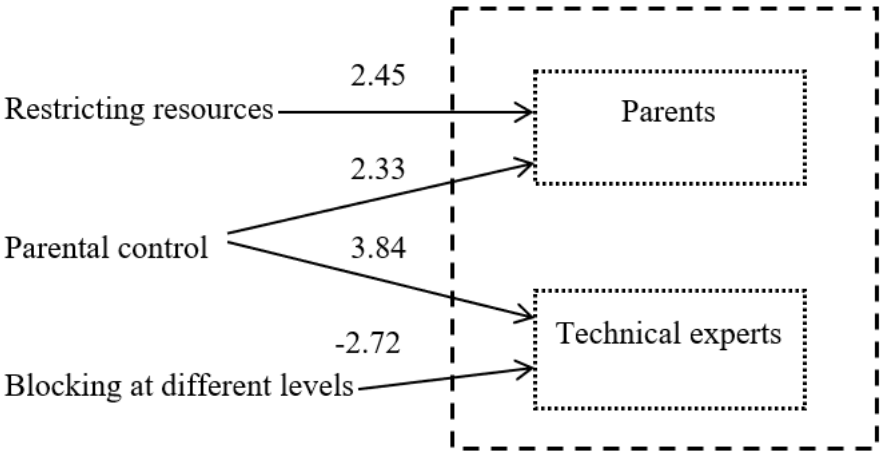

Figure 5.3: Determinants of Contributors to Child Online Safety

The parental control variable is influencing both parents, and technical experts initiated child online safety models. Therefore, the parents' control of children's online activities plays an important role in attaining online child safety. This can be performed by maintaining log records of online activities, installing supporting software, and permitting only genuine applications. Blocking at different levels is also an influencer of child online safety. This indicates blocking some unwanted information at different levels, including blocking through the apps on the device to blocking at ISP.

5.13. Conclusion

The demography and descriptive analysis of students, parents, technical experts, and legal experts are made in this chapter. Predictive analysis on parents and technical experts' opinions is performed to test some hypotheses. As a part of predictive analysis, different dependent and independent variables are identified through the literature review. Based on these identified variables, the different hypotheses on the prediction of parent and technical experts-initiated child online safety have been set. The regression analysis of the parent-initiated child online safety model shown that the variables restricting resources and parental control are the predictors of parent-initiated child online safety. Similarly, the technical experts-initiated child online safety model

regression result depicts that the variables blocking at different levels and parental control are the predictors of technical experts-initiated child online safety.

CHAPTER 6

DESIGN OF MODEL FOR CHILD ONLINE SAFETY USING SEM

6.1. Introduction

The chapter discusses the analysis of primary data and detailed interpretation of the results collected from technical experts. Technology experts are expected to suggest different measures to prevent online cybercrimes and exploitation of or on children. Responses can help to identify robust filtering or blocking concepts, content filtering and verification before content access, the role of Internet Service Providers, effective parental control mechanisms, and education requirements. The chapter discusses developed model for Child Online Safety and testing using Structural Equation Modeling (SEM). The chapter explains the various procedures and tests used for the analysis of the quality of primary data. The chapter also discusses the tests performed for testing the validity and reliability. The chapter provides the characteristics of the samples and describes a model for Online child safety. The study has established the interaction between the variables and developed a model. The important analysis is carried out before going for reliability and validity testing, including the tests for Quality of Primary data; Adequacy of sample size; Identification of missing values, and Identification of outliers. The chapter also includes a section for presenting the procedures used to test the measurement model's reliability and validity, including testing of convergent validity, discriminant validity, nomological validity, and face validity. Summation of scales is avoided by performing Confirmatory Factor Analysis (CFA). Construct validity explains to what extent the set of measured items reflect the corresponding theoretical latent construct they are supposed to measure. The chapter provides Convergent validity, Discriminant validity, Nomological validity, and Face validity and corresponding assessment by performing CFA/SEM for the latent constructs.

6.2. Analysis of Quality of Primary Data and Testing of Validity and Reliability

The section provides various procedures used in analyzing the quality of accumulated data for Child Online Safety. The section provides the tests performed for examining the validity and reliability. The primary data collected through questionnaires were subjected to robust quality evaluation. The data entered was examined for missing values and common errors by examining the descriptive statistics. Furthermore, the

reliability and validity of the study constructs were also checked for the constructs used for the study.

6.2.1. Quality Check- Primary Data

The quality of data collected is important in finding out the results of any research. Analysis and assuring the quality of gathered data are very important, which is the preface for data analysis. The activity includes measuring verification and cleaning further data analysis. The data collected through questionnaires have to be ensured for quality by performing certain benchmark tests. It includes sample size adequacy, missing value identification, and outlier identification.

Adequacy of Sample Size

A total of 287 respondents have been taken into consideration for primary data collection and 241 responses have been identified as valid and selected for the current analysis. Data set showed that constructs are having modest items commonalities and concern about sample size adequacy is fulfilled. Constructs with modest item commonalities (0.45-0.55) require a normal sample size of 200.

Identification of Missing Values

Missing values have much bearing on the results of any research study. Hence, these must be treated with utmost priority. If not handled with the procedural examination, the missing values can lead to facts being wrongly represented. One of the major reasons for missing values in survey data is no response from the respondents. The respondents may not answer all the questions due to various factors such as stress, lack of time.

The data entered was treated by examining the missing values and the common errors of data entry by closely checking the descriptive statistics. The absence of answers is considered as missing values. Out of the 287 responses, 46 are missing values. The questionnaires were given to 287 technical experts. Out of these 241, filled questionnaires were verified, checked, and matched manually. The responses were entered in Microsoft Excel and coded using SPSS 23.0 version. Data analysis was done using the Statistical Package for Social Sciences (SPSS) 23.0 version and Smart PLS 3. The measurement and structural models were evaluated to test the significance of the path estimates.

Identification of Outliers

Outliers are data point values that are distinctively different from other data point values in the data set. The outliers happen due to different reasons, such as coding errors, data entry errors, and certain unique values, which may happen due to unforeseeable circumstances. Normally, the outliers are identified by analyzing standard scores; samples with the smaller size the standardized variable values higher than 2.5. For larger samples, standardized variable values higher than four are considered (Hair et al., 2011). Observation in the current study is falling within the acceptable threshold, meeting the requirements. It was found that no cases corresponding to univariate outliers. Consequences of multivariate outliers are addressed by Mahalanobis D^2measure, as multivariate assessment of observations across the set of variables. Observations with a D^2/df value exceeding 2.5 in a smaller sample and 3 or 4 in a larger sample size are designated as possible outliers(Hair et al ,2011). The current study does not have any D^2/df above 2.5, and multivariate outliers are absent.

6.2.2. Testing of Validity and Reliability

Confirmatory Factor Analysis and Construct Validity

Summation of scales is kept away by carrying out Confirmatory Factor Analysis(CFA) as Structural Equation Modelling (SEM) programs determine factor scores for each respondent. CFA is used to examine "how well the variables represent a smaller number of constructs". In confirmatory factor analysis, "the researcher has to specify the number of factors on which the given variables converge and also specify which variables converge on which factors." The construct validity is defined as the degree to which a test measures what it claims, or purports, to be measuring." Construct validity ensures that the item measures from a sample represents the scores present in the population from which it is taken. Components of construct validity include: (i) Convergent validity,(ii)Discriminant validity, (iii) Nomological validity, and (iv) Face Validity and is measured by performing CFA/SEM(Hair et.al, 2011).

Convergent Validity

Convergent validity refers "to the degree to which two measures of constructs that theoretically should be related are related." Convergent validity, together with discriminant validity analysis, is a subtype of construct validity. Convergent validity

"can be established if two similar constructs correspond with one another, while discriminant validity applies to two dissimilar constructs that are easily differentiated" (Hair et al., 2011). Estimation of convergent validity is carried out using four different methods as follows.

(i) Factor Loadings

The values of factor loadings are an important criterion for determining convergent validity. High factor loading mentions that measured items converge towards a common point and indicate high convergent validity. Standardized loading estimates of 0.5 or high and an ideal value of factor loadings is 0.7 or high is identified as thumb rule concludes as a satisfactory convergent validity(Hair et al., 2011). The Square of standardized factor loading indicates what the latent factor illustrates extent variation in a measured item. Loading below 0.7 is considered significant(Hair et al., 2011).

(ii) Average Variance extracted

The average variance extracted(AVE) is the "amount of common variance among the latent construct indicators" (Hair et al., 2010), which is an indicator of convergent validity. It is calculated as the average value of squared factor loadings and is calculated using the formula 6.1.

Formula 6.1: Formula for calculating Average Variance Extracted

$$AVE = \frac{\sum_{i=1}^{n} \lambda_i^2}{n}$$

λ *stands for standaridised factor loading and i stands for the number of items*

For any item n, AVE is calculated as a sum of the squared standardized factor loadings by the total number of items. AVE with 0.5 indicates adequate convergence; any value less than 0.5 indicates more error in the identified items than the variance illustrated using the latent factor. It is highly urged that AVE be calculated for each latent construct part of the measurement model(Hair et al., 2011).

(iii) Reliability

Reliability is another indicator of Convergent validity. Reliability measures the internal consistency of the items. The reliability of the present study was analyzed using various reliability measures, namely Cronbach's alpha and Construct reliability (CR). An

accepted lower limit of Cronbach's alpha is 0.7 and can be minimum up to 0.6 for exploratory research. CR is computed using Formula 6.2.

Formula 6.2: Formula for Construct Reliability (CR)

$$CR = \frac{(\sum_{i=1}^{n} \lambda_i)^2}{\left(\sum_{i=1}^{n} \lambda_i\right)^2 + \left(\sum_{i=1}^{n} \delta_i\right)}$$

$$\lambda \, stands \, for \, standaridised \, factor \, loading, \delta \, stands \, for \, the \, error \, variance \, and \, i \, stands \, for \, the \, number \, of \, items$$

From Formula 6.1, CR is calculated as a value from the sum of factor loadings squared for each construct and the sum of the error variance terms.CR value 0.7 or higher indicates good reliability, and values between 0.6 and 0.7 are acceptable depending on whether the other construct validity indicators are satisfied or not. In the present study, all the values of CR are higher than the acceptance criteria.

(iv) R^2 Value

R^2 Values above 0.5 are identified as a strong indication for accepting reliability. Table 6.1 presents the indicators of convergent validity and corresponding acceptance levels (Hair et al., 2011).

Table 6.1: Indicators of Convergent Validity and Level of Acceptance

Category	*Acceptance Level*
Factor Loading	>= 0.5
AVE	>=0.5
Cronbach's Alpha-(Reliability)	>=0.7
Construct Reliability (CR)-(Reliability)	>=0.7
R^2-Reliability	>=0.5

Discriminant Validity

Discriminant validity or divergent validity tests degree towards a construct, and indicators deviate from another construct. Alternatively, the extent to which concepts or measurements are not supposed to be related is unrelated. Exogenous variables in the model are linked, and correlations between the variables are inspected. The correlation value between the exogenous variables not exceeding 0.85 indicates

acceptable discriminant validity(Zainudin, 2012). The more the exogenous variables are highly correlated, the more multicollinearity, which is not desirable. A high discriminant value is an indication that construct is unique in such a way that it is illustrating some processes which others cannot measure. Discriminant validity can be assessed using CFA. Discriminant validity can also be carried out by performing a series of $\chi 2$ difference tests. The presence of significant $\chi 2$ differences between all pairs of constructs indicates a piece of evidence for good discriminant validity (Bagozzi, Yi, and Philips, 1991). $\chi 2$ difference values are calculated by subtracting $\chi 2$ values of models unconstrained from constrained models, and values of 3.84 or above will be significant at the 0.05 level. The difference of 2 $\chi 2$ distributed values will always be $\chi 2$ distributed. The model with additional paths will be having a better fit based significant decrease in $\chi 2$Goodness of Fit. (Hair et al., 2011).

Nomological Validity

"Nomological validity is the degree that summated scales makes accurate predictions of other concepts in a theoretically based model" (Hair et al., 2011). Nomological validity is assessed using a correlation matrix. Items with summated scales are averaged, and a correlation matrix is analyzed to verify nomological validity.

Face Validity

Face validity or content validity is defined as the "assessment of the correspondence of the variables to be included in a summated scale and its conceptual definition"(Hair et al., 2011). A comprehensive list of items and constructs created by the items present in the instrument shall be created. Items and constructs are created using available kinds of literature reviewed. After the generation of variables, content validity shall be assured to make the instrument's statements understandable. In the current study, initial research instruments are given to experts from the industry for their suggestions.

Uni-dimensionality

Uni-dimensionality assessment is carried out using CFA and is significant for all key constructs (Li, S et al., 2005). CFA is used to identify how well the measured variables represent the construct (Hair et al., 2011). Uni-dimensionality is estimated using the CFA results. Recommended values for Standardized Root Mean Square Residual (SRMR) and Root Mean Square Error of approximation (RMSEA) values are below 0.08. Recommended threshold value for Goodness of Fit (GFI), Adjusted Goodness of

Fit (AGFI), Normal Fit Index (NFI), Incremental Fit Index (IFI), Tucker Lewis Index (TLI), and Comparative Fit Index Value (CFI) is 0.90(Hair et al., 2011). Further data fitness of the hypothesized model is also verified by using CFA along with other assessments. Model fit indices are classified as absolute fit, incremental fit, and parsimonious fit. Redundant items present in the model are constrained. Table 6.2 provides the Fitness of Indices (Hair et al., 2011; Hooper et al., 2008; Bentler, 2009).

Table 6.2: Fitness Indices

Category	*Index*	*Acceptance Level*
Chi-Square/DF	CMIN/DF	<5.0
Absolute Fit	Model Chi-Square(**χ2**)	>0.05
	Standardized Root Mean Square Residual (SRMR)	<0.08
	Goodness-of-fit (GFI)	>0.9
	Adjusted Goodness-of-fit (AGFI)	>0.9
	Root Mean Square Error of Approximation (RMSEA)	<0.08
Incremental Fit	Normed-fit-Index (NFI)	>0.9
	Incremental Fit Index (IFI)	>0.9
	Tucker Lewis Index (TLI)	>0.9
	Comparative Fit Index (CFI)	>0.9

6.3. Validity and Reliability Testing for Child Online Safety

The current study, individual Confirmatory Factor Analysis (CFA), is carried out by considering latent constructs one by one.

6.3.1 Confirmatory Factor Analysis for Latent Construct- Establishing Wanted Contact

Table 6.3 provides the item description of the latent construct WC. Item WC1 is used for analyzing how avoidance of unwanted contact can reduce the risk of cyber solicitation and allied crime. WC2 correspond to how reducing unwanted online habit avoids cybercrime significantly. WC3 examines Confining children to the home and

furnishing them with media and technology that will make the child's bedroom a more attractive alternative to the apparent dangers of the outside world. WC4 validates whether providing auto information exchange for web access can help prohibit children from contacting bullying elements or groomers to avoid cyber children exploitation or blackmailing. WC5 corresponds to exploiting demographic information such as location, age, previous search patterns, and allied user personalization variables to help update parents and children to avoid unwanted (harmful) contacts.

Table 6.3: Latent Construct WC- Item Description

Variable Name	Item Description	Item Id
WC	Avoiding unwanted contact	WC1
	Reducing unwanted online habit	WC2
	Confining children to the home	WC3
	Providing auto information exchange for web-access	WC4
	Exploiting demographic information	WC5

Figure 6.1 shows the summary of Confirmatory Factor Analysis for Latent Construct – WC. Table 6.4 represents statistical representation of the latent construct WC with calculated mean and standard deviation. The table also provides the frequency, percentage, and cumulated frequency related to each item and corresponding responses. Tables 6.5 and 6.6 present the fitness indices and reliability and validity measures of the construct Establishing Wanted Contact.

Table 6.4: Latent Construct WC- Statistical Representation

Item Id	Mean	Std. Dev	SD			D			N			A			SA		
			F	%	C%	F	%	C%	F	%	C%	F	%	C%	F	%	C%
WC1	3.1	1.26	26	10.8	10.8	57	23.7	34.5	67	27.8	62.3	48	19.9	82.2	43	17.8	100
WC2	3.15	1.22	25	10.4	10.4	50	20.7	31.1	67	27.8	58.9	61	25.3	84.2	38	15.8	100
WC3	3.09	1.23	28	11.6	11.6	51	21.2	32.8	69	28.6	61.4	57	23.7	85.1	36	14.9	100
WC4	3.07	1.24	29	12	12	55	22.8	34.8	62	25.7	60.6	61	25.3	85.9	34	14.1	100
WC5	3.17	1.16	22	9.1	9.1	46	19.1	28.2	76	31.5	59.8	64	26.6	86.3	33	13.7	100

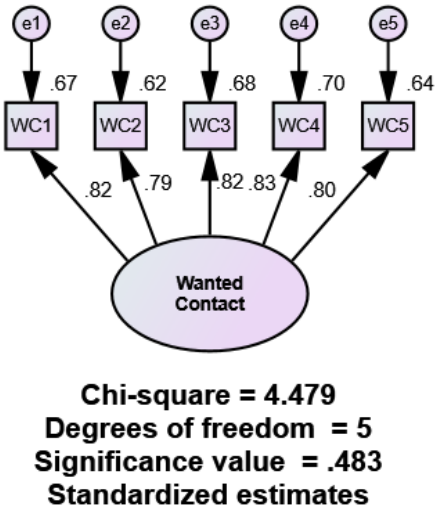

Figure 6.1: CFA Summary for Latent Construct- WC

Table 6.5: Latent Construct WC-Fitness Index representation

Variable Name	CMIN/ DF	χ2	SRMR	GFI	AGFI	RMSEA	NFI	IFI	TLI	CFI
WC	.896	4.479	.018	.993	.979	.000	.994	1.0001	1.001	1.000

Convergent Validity Analysis

Table 6.6 shows the convergent validity representation of the construct Establishing Wanted Contact (WC). WC1 has statistically significant ($p < 0.001$) factor loading of .821, WC2 with statistically significant ($p < 0.001$) factor loading of .786, WC3 with statistically significant ($p < 0.001$) factor loading of .824, WC4 with statistically significant ($p < 0.001$) factor loading of .835 and WC5 with statistically significant ($p < 0.001$) factor loading of .797. From the summary given in the table, it can be observed that all indicators (WC1, WC2, WC3, WC4, WC5) of Establishing Wanted Contact have statistically significant ($p < 0.001$) factor loadings from in the range 0.786 to 0.835, which is an indication of good convergent validity of the construct. Additionally, Table 6.6 provides the Average Variance Extracted (AVE) of the construct WC with a value of 0.661, exceeding the suggested minimum value of 0.50, indicating strong convergent validity. Cronbach's Alpha Value and Composite Reliability Value for the construct WC are 0.907 and 0.907, respectively, above the recommended value of 0.70, indicating that measurement scales are adequately reliable. R2 values are in the range of 0.619 to 0.697, which is above 0.5 is clear evidence for acceptable reliability. Results provide strong evidence that the latent construct Establishing Wanted Contact has adequate convergent validity.

Uni-dimensionality Analysis

The uni-dimensionality of the latent construct WC can be estimated from the CFA results shown in Table 6.5. The value for SRMR is 0.018, and RMSEA is 0.000. Derived values of SRMR and RMSEA values are below the recommended value of 0.08. Additionally, the table provides the values, GFI of 0.993, AGFI of 0.979, NFI of 0.994, IFI of 1.0001, TLI of 1.001, and CFI of 1.000. It is visible that that shown values in the table are above the recommended threshold of 0.90. Results shown in the table prove the uni-dimensionality of the latent construct Establishing Wanted Contact (WC). There are no cross-loadings, and all the identified indicators reflect only one construct: Establishing Wanted Contact (WC).

Table 6.6: Validity and Reliability Testing of Latent Construct WC

Variable	**Items**	**Standardized Regression Weight (**Factor Loadings)	**Average Variance Extracted**	**Cronbach's Alpha**	**Composite Reliability**	**Squared Multiple Correlations**
WC	WC1	.821	.661	.907	.907	.675
	WC2	.786				.619
	WC3	.824				.679
	WC4	.835				.697
	WC5	.797				.636

6.3.2 Confirmatory Factor Analysis for Latent Construct- Content Filtering

Table 6.7 provides the item description of the latent construct CF. Item CF1 is used to analyze how strict content Monitoring and filtering (URL, content search, keyword, demographic sensitive filtering) approach is effective in avoiding pornography and allied online children exploitation cases. CF2 Providing predefined or dedicated e-learning media such as mobile and computer with predefined content filtering provision and log detail auto-update can help avoid kids to incline in the negative direction. CF3 examines how content-sensitive session control and content-filtering can effectively avoid cyber children crime (online fraud/cheating/blackmailing/threat). CF4 validates whether enabling content block provision with internet service providers can help curb child online exploitation or harassment. CF5 corresponds to providing a link-block option with browser to avoid accidentally seen pornographic contents forwarded by else can curb child online harassment or bullying

Table 6.7: Latent Construct CF- Item Description

Variable Name	Item Description	Item Id
CF	Strict content Monitoring and filtering (URL, content search, keyword, demographic sensitive filtering)	CF1
	Providing predefined or dedicated e-learning media such as mobile and computer with predefined content filtering provision	CF2
	Content-sensitive session control to avoid cyber children crime (online fraud/cheating/blackmailing/threat)	CF3
	Enabling content block provision with the internet service provider	CF4
	Providing link-block option with browser to avoid accidentally seen pornographic contents forwarded by else	CF5

Figure 6.3 shows the summary of Confirmatory Factor Analysis for Latent Construct – CF. Table 6.8 represents the statistical representation of the latent construct CF with calculated mean and standard deviation. The table also provides the frequency, percentage, and cumulated frequency related to each item and corresponding responses. Tables 6.9 and 6.10 present the fitness indices and reliability and validity measures of the construct Content Filtering.

Table 6.8: Latent Construct CF- Statistical Representation

Item Id	Mean	Std Dev.	SD			D			N			A			SA		
			F	%	C%	F	%	C%	F	%	C%	F	%	C%	F	%	C%
CF1	3.15	1.217	21	8.7	8.7	57	23.7	32.4	69	28.6	61	52	21.6	82.6	42	17.4	100
CF2	3.13	1.217	24	10	10	53	22	32	70	29	61	55	22.8	83.8	39	16.2	100
CF3	3.12	1.254	30	12.4	12.4	46	19.1	31.5	70	29	60.6	55	22.8	83.4	40	16.6	100
CF4	3.13	1.24	31	12.9	12.9	42	17.4	30.3	69	28.6	58.9	63	26.1	85.1	36	14.9	100
CF5	3.1	1.254	28	11.6	11.6	52	21.6	33.2	71	29.5	62.7	48	19.9	82.6	42	17.4	100

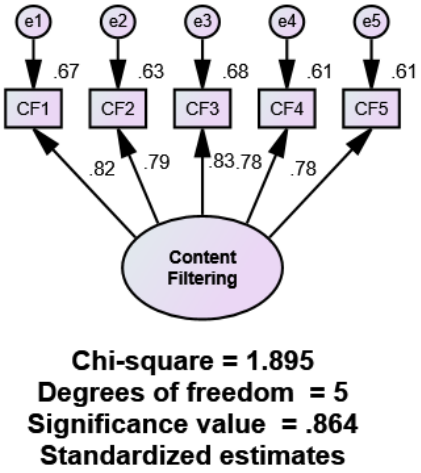

Figure 6.2: CFA Summary for Latent Construct- CF

Table 6.9: Latent Construct CF-Fitness Index representation

Variable Name	CMIN/ DF	χ2	SRMR	GFI	AGFI	RMSEA	NFI	IFI	TLI	CFI
CF	.379	1.895	.013	.997	.990	.000	.997	1.0005	1.009	1.000

Convergent Validity Analysis

Table 6.10 shows the convergent validity representation of the construct Content Filtering (CF). CF1 has statistically significant ($p < 0.001$) factor loading of .821, CF2 with statistically significant ($p < 0.001$) factor loading of .793, CF3 with statistically significant ($p < 0.001$) factor loading of .825, CF4 with statistically significant ($p < 0.001$) factor loading of .781 and CF5 with statistically significant ($p < 0.001$) factor loading of .778. From the summary given in the table, it can be observed that all indicators (CF1, CF2, CF3, CF4, CF5) for Content Filtering have statistically significant ($p < 0.001$) factor loadings from in the range 0.778 to 0.825, which is an indication of good convergent validity of the construct. Additionally, Table 6.10 provides the Average Variance Extracted (AVE) of the construct CF with a value of 0.676 the suggested minimum value of 0.50, which indicates Cronbach's Alpha Value and Composite Reliability Value for the construct CF is 0.899 and 0.899, respectively, which is above the recommended value of 0.70, indicating that measurement scales are adequately reliable. R2 values are in the range 0.605 to 0.681, which is above 0.5 is a shred of clear evidence for acceptable reliability. Results provide strong evidence that latent construct Content Filtering has adequate convergent validity.

Table 6.10: Validity and Reliability Testing of Latent Construct CF

Variable	Items	Standardized Regression Weight (Factor Loadings)	Average Variance Extracted	Cronbach's Alpha	Composite Reliability	Squared Multiple Correlations
CF	CF1	.821	.676	.899	.899	.674
	CF2	.793				.629
	CF3	.825				.681
	CF4	.781				.610
	CF5	.778				.605

Uni-dimensionality Analysis

The uni-dimensionality of the latent construct CF can be estimated from the CFA results shown in Table 6.9. The value for SRMR is 0.013, and RMSEA is 0.000. Derived values of SRMR and RMSEA values are below the recommended value of 0.08. Additionally, the table provides the values, GFI of 0.997, AGFI of 0.990, NFI of 0.997, IFI of 1.0005, TLI of 1.009, and CFI of 1.000. It is visible that that shown values in the table are above the recommended threshold 0.90. Results shown in the table prove the uni-dimensionality of the latent construct Content Filtering (CF). Obviously, there are no cross loadings, and all the identified indicators reflect only one construct: Content Filtering (CF).

6.3.3 Confirmatory Factor Analysis for Latent Construct-Identification Systems

Table 6.11 provides the item description of the latent construct IS. Item IS1 corresponds to monitoring the log details of kids and their socio-behavioral changes throughout internet access or after using internet access. IS2 examines whether enabling anti-recording or replication features when making online communication through video calling or multimedia sharing can help avoiding online child abuse, blackmailing, and exploitation. IS3 examines how spatial and temporal relationships between offenders can help identify possible offenders. IS4 validates whether the identification of commercial market and its circuit can help in prohibiting children online sexual exploitation or allied events. IS5 examines whether ICT can help human traffickers recruit new victims, including children, and market child sex tourism. Hence, identifying such activities using web-mining and personalization can help eradicate such issues.

Table 6.11: Latent Construct IS- Item Description

Variable Name	Item Description	Item Id
IS	Monitoring log details of kids and their socio-behavioral changes during or after internet access	IS1
	Enabling anti-recording or replication features when making online communication through video calling or multimedia sharing	IS2
	Exploiting spatial and temporal relationship between offenders in identifying the possible offender	IS3
	Identification of commercial market and its circuit for prohibiting children online sexual exploitation or allied events	IS4
	Identifying human traffickers activities using web-mining and personalization for eradication	IS5

Figure 6.3 shows the summary of Confirmatory Factor Analysis for Latent Construct – IS. Table 6.12 represents the statistical representation of the latent construct IS with calculated mean and standard deviation. The table also provides the frequency, percentage and cumulated frequency related to each item and corresponding responses. Tables 6.13 and 6.14 present the fitness indices and reliability and validity measures of the construct Identification Systems.

Table 6.12: Latent Construct IS- Statistical Representation

Item Id	Mean	Std Dev	SD			D			N			A			SA		
			F	%	C%	F	%	C%	F	%	C%	F	%	C%	F	%	C%
IS1	3.23	1.285	24	10	10	51	21.2	31.1	66	27.4	58.5	46	19.1	77.6	54	22.4	100
IS2	3.18	1.248	24	10	10	51	21.2	31.1	69	28.6	59.8	51	21.2	80.9	46	19.1	100
IS3	3.1	1.2	25	10.4	10.4	54	22.4	32.8	67	27.8	60.6	62	25.7	86.3	33	13.7	100
IS4	3.16	1.225	21	8.7	8.7	59	24.5	33.2	64	26.6	59.8	55	22.8	82.6	42	17.4	100
IS5	3.18	1.274	28	11.6	11.6	45	18.7	30.3	72	29.9	60.2	48	19.9	80.1	48	19.9	100

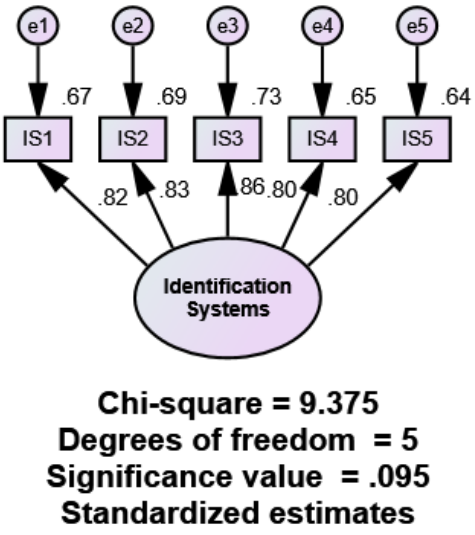

Figure 6.3: CFA Summary for Latent Construct- IS

Table 6.13: Latent Construct IS-Fitness Index representation

Variable Name	CMIN/DF	χ^2	SRMR	GFI	AGFI	RMSEA	NFI	IFI	TLI	CFI
IS	1.875	9.375	0.026	0.984	0.953	0.06	0.988	0.994	0.989	0.994

Convergent Validity Analysis

Table 6.14 shows the convergent validity representation of the construct Identification Systems (IS). IS1 has statistically significant ($p < 0.001$) factor loading of .820, IS2 with statistically significant ($p < 0.001$) factor loading of .828, IS3 with statistically significant ($p < 0.001$) factor loading of .856, IS4 with statistically significant ($p < 0.001$) factor loading of .803 and IS5 with statistically significant ($p < 0.001$) factor loading of .802. From the summary given in the table, it can be observed that all indicators (IS1, IS2, IS3, IS4, IS5) for Identification Systems have statistically significant ($p < 0.001$) factor loadings from in the range 0.802 to .856, which is an indication of good convergent validity of the construct. Additionally, Table 6.14 provides the Average Variance Extracted (AVE) of the construct CF with a value of 0.640, exceeding the suggested minimum value of 0.50, indicating strong convergent validity. Cronbach's Alpha Value and Composite Reliability Value for the construct IS are 0.912 and 0.912, respectively, above the recommended value of 0.70, indicating that measurement scales are adequately reliable. R2 values are in the range 0.643 to 0.733, which is above 0.5 is a shred of clear evidence for acceptable reliability. Results provide strong evidence that latent construct Identification Systems have adequate convergent validity.

Table 6.14: Validity and Reliability Testing of Latent Construct IS

Variable	Items	Standardized Regression Weight (Factor Loadings)	Average Variance Extracted	Cronbach's Alpha	Composite Reliability	Squared Multiple Correlations
IS	IS1	.820	.676	.912	.912	.672
	IS2	.828				.685
	IS3	.856				.733
	IS4	.803				.645
	IS5	.802				.643

Uni-dimensionality Analysis

The uni-dimensionality of the latent construct IS can be estimated from the CFA results shown in Table 6.13. The value for SRMR is 0.026, and RMSEA is 0.060. Derived values of SRMR and RMSEA values are below the recommended value of 0.08. Additionally, the table provides the values, GFI of 0.984, AGFI of 0.953, NFI of 0.988, IFI of .994, TLI of .989, and CFI of .994. It is visible that that shown values in the table are above the recommended threshold of 0.90. Results shown in the table prove the uni-dimensionality of the latent construct Identification Systems (IS). There are no cross loadings, and all the identified indicators reflect only one construct Identification system (IS).

6.3.4 Confirmatory Factor Analysis for Latent Construct –Parental Control and Education Awareness (PE)

Table 6.15 provides the item description of the latent construct PE. Item PE1 is used for examining how frequent search pattern filtering and parental control can be an effective solution. PE2 examines how parental control software restricts app installation or use can be a robust solution. PE3 validates parental control features and capability for blocking, restricting, limiting, or allowing access to different features for younger children. PE4 tries to identify which circumstances pose what kind of risk, which factors mean that risk is increased or reduced, and when risks do or do not result in tangible harm can avoid cyber child abuse help in curbing online child exploitation. PE5 examines avoiding third-party applications from auto-download and media access without permission can help to avoid personal data loss and further defamation. PE6 corresponds to how cyber-bullies using public websites and social media to broaden their audience and increase the impact on victims and how detecting the events can be vital.

Table 6.15: Latent Construct PE- Item Description

Variable Name	Item Description	Item Id
PE	Frequent search pattern filtering and parental control can be an effective solution	PE1
	Parental control software to restrict app installation or use can be a vital solution	PE2
	Parental control features with the capability for blocking, restricting, limiting, or allowing access to different features for younger children	PE3
	Identifying circumstances posing a risk, factors for risk rise or decrease, when risks do or do not result in tangible harm can avoid cyber child abuse	PE4
	Avoiding third-party applications from auto-download and media (phone data) access without permission can help to avoid private data loss and further defamation	PE5
	Cyber-bullies may use public websites and social media to broaden their audience and increase the impact on victims and hence detecting such events can be vital	PE6

Figure 6.4 shows the summary of Confirmatory Factor Analysis for Latent Construct – PE. Table 6.16 represents a statistical representation with calculated mean and standard deviation. The table also provides the frequency, percentage, and cumulated frequency related to each item and corresponding responses. Tables 6.17 and 6.18 present the fitness indices and reliability and validity measures of the construct IS.

Table 6.16: Latent Construct PE- Statistical Representation

Item Id	Mean	Std Dev	SD			D			N			A			SA		
			F	%	C%	F	%	C%	F	%	C%	F	%	C%	F	%	C%
PE1	3.15	1.146	26	10.8	10.8	37	15.4	26.1	79	32.8	58.9	72	29.9	88.8	27	11.2	100
PE2	3.08	1.277	33	13.7	13.7	50	20.7	34.4	61	25.3	59.8	59	24.5	84.2	38	15.8	100
PE3	3.13	1.146	20	8.3	8.3	52	21.6	29.9	78	32.4	62.2	59	24.5	86.7	32	13.3	100
PE4	3.11	1.255	27	11.2	11.2	54	22.4	33.6	67	27.8	61.4	51	21.2	82.6	42	17.4	100
PE5	3.02	1.207	34	14.1	14.1	46	19.1	33.2	65	27	60.2	72	29.9	90	24	10	100
PE6	3.1	1.279	28	11.6	11.6	56	23.2	34.9	65	27	61.8	47	19.5	81.3	45	18.7	100

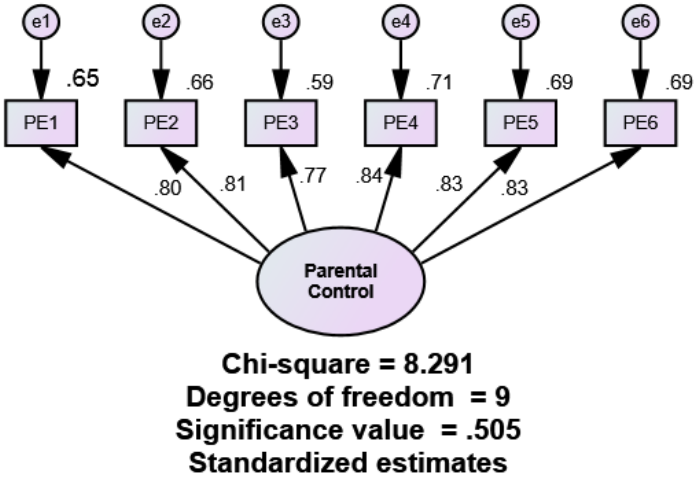

Figure 6.4: CFA Summary for Latent Construct- PE

Table 6.17: Latent Construct PE-Fitness Index representation

Variable	CMIN/ DF	χ2	SRMR	GFI	AGFI	RMSEA	NFI	IFI	TLI	CFI
PE	.921	8.291	.020	.988	.973	.000	.991	1.001	1.001	1.000

Convergent Validity Analysis

Table 6.18 shows the convergent validity representation of the construct Parental control and Education Awareness. PE1 has statistically significant ($p < 0.001$) factor loading of .805, PE2 with statistically significant ($p < 0.001$) factor loading of .814, PE3 with statistically significant ($p < 0.001$) factor loading of .768, PE4 with statistically significant ($p < 0.001$) factor loading of .841, PE5 with statistically significant ($p < 0.001$) factor loading of .830 and PE6 with statistically significant ($p < 0.001$) factor loading of .829 . From the summary given in the table, it can be observed that all indicators (PE1, PE2 PE3, PE4, PE5, PE6) for Parental Control and Education Awareness have statistically significant ($p < 0.001$) factor loadings from in the range 0.768 to .841 which is an indication of good convergent validity of the construct. Additionally, Table 6.14 provides the Average Variance Extracted (AVE) of the construct PE with a value of 0.664, exceeding the suggested minimum value of 0.50, indicating strong convergent validity. Cronbach's Alpha Value and Composite Reliability Value for the construct IS are 0.922 and 0.922, respectively, above the recommended value of 0.70, indicating that measurement scales are adequately reliable. R2 values are in the range 0.589 to 0.708, which is above 0.5 is a shred of clear evidence

for acceptable reliability. Results provide strong evidence that the latent construct Parental Control and Education Awareness has adequate convergent validity.

Table 6.18: Validity and Reliability Testing of Latent Construct PE

Variable	Items	Standardized Regression Weight (Factor Loadings)	Average Variance Extracted	Cronbach's Alpha	Composite Reliability	Squared Multiple Correlations
PE	PE1	.805	.664	.922	.922	.648
	PE2	.814				.662
	PE3	.768				.589
	PE4	.841				.708
	PE5	.830				.689
	PE6	.829				.688

Uni-dimensionality Analysis

The uni-dimensionality of the latent construct IS can be estimated from the CFA results shown in Table 6.17. The value for SRMR is 0.020, and RMSEA is 0.000. Derived values of SRMR and RMSEA values are below the recommended value of 0.08. Additionally, the table provides the values, GFI of 0.988, AGFI of 0.973, NFI of 0.991, IFI of 1.001, TLI of 1.001, and CFI of 1.000. It is visible that shown values in the table are above the recommended threshold of 0.90. Results shown in the table prove the uni-dimensionality of the latent construct Parental Control and Education Awareness(PE). There are no cross loadings, and all the identified indicators reflect only one construct: Parental Control and Education Awareness (PE).

6.3.5 Confirmatory Factor Analysis for Latent Construct–ISP Level Efforts(IL)

Table 6.19 provides the item description of the latent construct PE. Item IL1 is used for examining the effect of filters or parental control installation on an individual computer and configuring at the ISP level. IL2examines the effectiveness of ISPs in blocking content originating from specific IP addresses found to be distributing child abuse images. IL3 validates inducing the ability or justification of ISPs to determine whether the content was illegal, and the block list's transparency can help avoid online children exploitation.

Figure 6.5 shows the summary of Confirmatory Factor Analysis of for Latent Construct –IL. Table 6.20 represents statistical representation of the latent construct IL with calculated mean and standard deviation. Table also provides the frequency, percentage and cumulated frequency related to each of the items and corresponding responses.

Tables 6.21 and 6.22 present the fitness indices and reliability and validity measures of the construct Identification Systems.

Table 6.19: Latent Construct IL- Item Description

Variable Name	Item Description	Item Id
IL	Filters or parental control installation on individual computers and configuration at ISP Level	IL1
	Bocking content originating from specific IP address that distributes child abuse images	IL2
	Ability or justification for ISPs to determine legality of content and transparency of block lists for avoiding online child exploitation	IL3

Table 6.20: Latent Construct PE- Statistical Representation

Item Id	Mean	Std Dev	SD			D			N			A			SA		
			F	%	C%	F	%	C%	F	%	C%	F	%	C%	F	%	C%
IL1	3.2	1.197	22	9.1	9.1	48	19.9	29	71	29.5	58.5	61	25.3	83.8	39	16.2	100
IL2	3.15	1.144	21	8.7	8.7	49	20.3	29	75	31.1	60.2	66	27.4	87.6	30	12.4	100
IL3	3.17	1.234	24	10	10	54	22.4	32.4	61	25.3	57.7	62	25.7	83.4	40	16.6	100

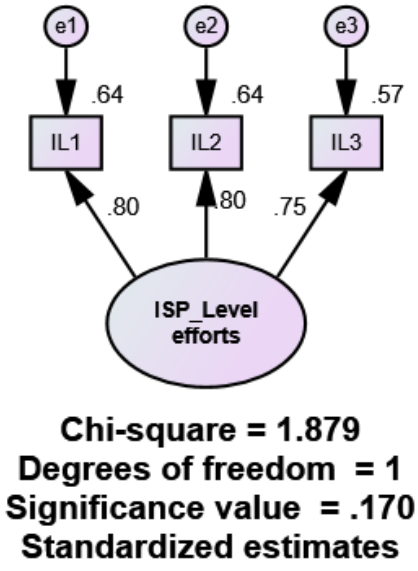

Figure 6.5: CFA Summary for Latent Construct- IL

Table 6.21: Latent Construct IL-Fitness Index representation

Variable Name	CMIN /DF	χ2	SRMR	GFI	AGFI	RMSEA	NFI	IFI	TLI	CFI
IL	1.879	1.879	.047	.995	.969	.061	.993	0.997	.990	.997

Convergent Validity Analysis

Table 6.22 shows the convergent validity representation of the construct ISP Level Efforts. IL1 has statistically significant ($p < 0.001$) factor loading of .799, IL2 with statistically significant ($p < 0.001$) factor loading of .799 and IL3 with statistically significant ($p < 0.001$) factor loading of .755. From the summary given in the table, it can be observed that all indicators (IL1, IL2, IL3) for ISP Level Efforts have statistically significant ($p < 0.001$) factor loadings from in the range 0.755 to .799, which is an indication of good convergent validity of the construct. Additionally, Table 6.22 provides the Average Variance Extracted (AVE) of the construct IL with a value of 0.616, exceeding the suggested minimum value of 0.50, indicating strong convergent validity. Cronbach's Alpha Value and Composite Reliability Value for the construct IL is 0.827 and 0.828, respectively, above the recommended value of 0.70, indicating that measurement scales are adequately reliable. R2 values are in the range 0.570 to 0.639, which is above 0.5 is a piece of clear evidence for acceptable reliability. Results provide strong evidence that latent construct ISP Level Efforts has adequate convergent validity.

Table 6.22: Validity and Reliability Testing of Latent Construct PE

Variable	Items	Standardized Regression Weight (Factor Loadings)	Average Variance Extracted	Cronbach's Alpha	Composite Reliability	Squared Multiple Correlations
IL	IL1	.799	.616	.827	.828	.639
	IL2	.799				.639
	IL3	.755				.570

Uni-dimensionality Analysis

The uni-dimensionality of the latent construct IL estimated from the CFA results is shown in Table 6.22. The uni-dimensionality of the latent construct IL can be estimated from the CFA results shown in Table 6.21. The value for SRMR is 0.047, and RMSEA is 0.061. Derived values of SRMR and RMSEA values are below the recommended value of 0.08. Additionally, the table provides the values, GFI of 0.995, AGFI of 0.969,

NFI of 0.993, IFI of .997, TLI of .990, and CFI of .997. It is visible that shown values in the table are above the recommended threshold 0.90. Results shown in the table prove the uni-dimensionality of the latent construct ISP Level Efforts (IL). There are no cross-loadings, and all the identified indicators reflect only one construct, ISP Level Efforts(IL).

6.3.6 Confirmatory Factor Analysis - Latent Construct Child Online Safety(CS)

Figure 6.6 shows the summary of Confirmatory Factor Analysis of Latent Construct CS.

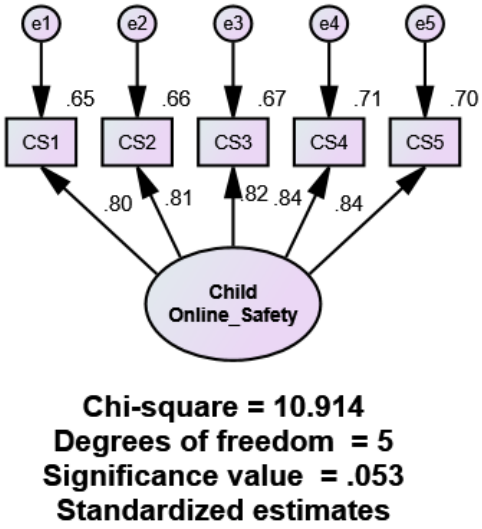

Figure 6.6: CFA Summary for Latent Construct- CS

Tables 6.24 and 6.25 present the fitness indices and reliability and validity measures of the construct Child Online Safety(CS). Table 6.23 represents statistical representation of the latent construct CS with calculated mean and standard deviation. The table also provides the frequency, percentage, and cumulated frequency related to each item and corresponding responses.

Convergent Validity Analysis

Table 6.25 shows the convergent validity representation of the construct Child Online Safety. Table 6.25 shows the convergent validity representation of Child Online Safety(CS). CS1has statistically significant ($p < 0.001$) factor loading of .804, CS2 with statistically significant ($p < 0.001$) factor loading of .812 , CS3 with statistically significant ($p < 0.001$) factor loading of .821, CS4 with statistically significant ($p < 0.001$) factor loading of .841 and CS5 with statistically significant ($p < 0.001$) factor loading of .838. From the summary given in the table, it can be observed that all indicators (CS1, CS2, CS3, CS4, CS5) for Child Online Safety have statistically

significant ($p < 0.001$) factor loadings from in the range 0.804 to .841, which is an indication of good convergent validity of the construct. Additionally, table 6.25 provides the Average Variance Extracted (AVE) of the construct CS with a value of 0.678, exceeding the suggested minimum value of 0.50, indicating strong convergent validity. Cronbach's Alpha Value and Composite Reliability Value for the construct CS is 0.913 and 0.913, respectively, above the recommended value of 0.70, indicating that measurement scales are adequately reliable. R2 values are in the range 0.646 to 0.707, which is above 0.5 is a piece of clear evidence for acceptable reliability. Results provide strong evidence that the latent construct Child Online Safety has adequate convergent validity.

Table 6.23: Latent Construct CS- Statistical Representation

Item Id	Mean	Std Dev	SD			D			N			A			SA		
			F	%	C%	F	%	C%	F	%	C%	F	%	C%	F	%	C%
CS1	3.2	1.214	21	8.7	8.7	51	21.2	29.9	73	30.3	60.2	52	21.6	81.7	44	18.3	100
CS2	3.03	1.234	29	12	12	57	23.7	35.7	67	27.8	63.5	53	22	85.5	35	14.5	100
CS3	3.13	1.213	23	9.5	9.5	55	22.8	32.4	70	29	61.4	54	22.4	83.8	39	16.2	100
CS4	3.12	1.295	30	12.4	12.4	52	21.6	34	66	27.4	61.4	46	19.1	80.5	47	19.5	100
CS5	3.04	1.261	31	12.9	12.9	52	21.6	34.4	75	31.1	65.6	42	17.4	83	41	17	100

Table 6.24: Latent Construct CS- Fitness Index Representation

Variable Name	CMIN/ DF	$\chi 2$	SRMR	GFI	AGFI	RMSEA	NFI	IFI	TLI	CFI
CS	2.183	10.914	.026	.984	.95	.070	.986	0.992	.985	.992

Table 6.25: Validity and Reliability of Latent Construct CS

Variable	Items	Standardized Regression Weight (Factor Loadings)	Average Variance Extracted	Cronbach's Alpha	Composite Reliability	Squared Multiple Correlations
CS	CS1	.804	.678	.913	.913	.646
	CS2	.812				.659
	CS3	.821				.675
	CS4	.841				.707
	CS5	.838				.702

Uni-dimensionality Analysis

The uni-dimensionality of the latent construct CS can be estimated from the CFA results shown in Table 6.24. The value for SRMR is 0.026, and RMSEA is 0.070. Derived values of SRMR and RMSEA values are below the recommended value of 0.08. Additionally, the table provides the values, GFI of 0.984, AGFI of 0.951, NFI of 0.986, IFI of .992, TLI of .985, and CFI of .992. It is visible that shown values in the table are

above the recommended threshold of 0.90. Results shown in the table prove the uni-dimensionality of the latent construct Child Online Safety(CS). There are no cross loadings, and all the identified indicators reflect only one construct, Child Online Safety(CS).

6.3.7 Discriminant Validity Analysis

Researchers established the discriminant validity by examining the correlation between the exogenous variables and verified that values are less than 0.85(Zainudin, 2012). Figure 6.7 shows the result of pooled CFA for Child Online Safety. Table 6.26 provides exogenous constructs and corresponding inter-correlation values.

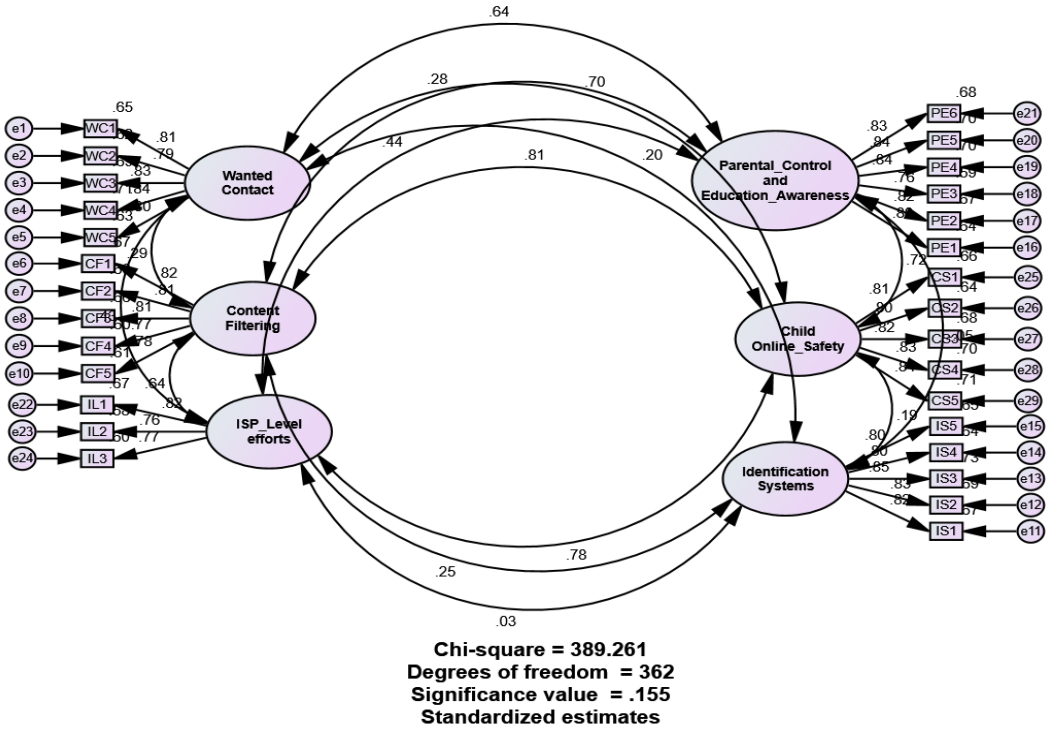

Figure 6.7: Result of pooled CFA for Child Online Safety

Table 6.26: Exogenous Constructs and their inter-correlation values

Constructs	Inter Correlation					
	WC	CF	IS	PE	IL	CS
WC	1					
CF	.289	1				
IS	.201	.255	1			
PE	.643	.053	.053	1		
IL	.434	.033	.033	.444	1	
CS	.699	.807	.188	.721	.778	1

6.3.8 Nomological Validity

Nomological validity is verified using the correlation matrix. Items comprising the summated scale are summed and the correlation matrix is examined. Table 6.27 shows the correlation between the constructs which indicate acceptable nomological validity.

Table 6.27: Correlation of the Constructs – Child Online Safety

Correlations							
		SUM_WC	SUM_CF	SUM_IS	SUM_PE	SUM_IL	SUM_CS
SUM_WC	Pearson Correlation	1	.255**	.184**	.585**	.372**	.635**
SUM_CF	Pearson Correlation	.255**	1	.232**	.254**	.555**	.728**
SUM_IS	Pearson Correlation	.184**	.232**	1	-.049	.027	.171**
SUM_PE	Pearson Correlation	.585**	.254**	-.049	1	.387**	.662**
SUM_IL	Pearson Correlation	.372**	.555**	.027	.387**	1	.677**
SUM_CS	Pearson Correlation	**.635****	**.728****	**.171****	**.662****	**.677****	1
**. Correlation is significant at the 0.01 level (2-tailed).							

6.3.9 Face Validity

Initially generated research instruments were given to industry experts and practitioners for their comments and suggestions. Comments and suggestions were accepted and included in the refined research instrument for ensuring face validity.

6.3.10 Result Summary of Validity and Reliability Testing of Child Online Safety

Section 6.2 of the chapter discussed the procedures used in testing the reliability and validity of the measurement model of Child Online Safety, including (i)convergent validity; (ii)uni-dimensionality; (iii) discriminant validity; (iv) nomological validity; and (v) face validity. Convergent validity and uni-dimensionality were examined using individual Confirmatory Factor Analysis. Convergent validity and uni-dimensionality were established using CFA. Results have shown that all the latent constructs are having adequate levels of convergent validity. Also, individual CFA results proved that latent constructs are unidimensional. Checking inter-correlation values of exogenous constructs below 0.85 has been taken as evidence for discriminant validity. The nomological validity of the study was established using the correlation matrix of the constructs, and face validity was carried out using expert recommendations. It is concluded that the validity and reliability of all the constructs of Child Online Safety were established very well.

6.4 Causal Model and Hypothesis Testing

This section describes the details of hypothesis testing Structural Equation Modelling, which consists of two parts;(i) Measurement model for ensuring the instrument's validity and reliability, which was covered in the previous section (ii) structural model along with empirical results.

6.4.1. Structural Equation Modelling (SEM)

Structural Equation Modelling (SEM) is classified as a statistical model for attaining relationships among multiple variables." SEM examines the structure of interrelationships expressed in a series of equations, similar to a series of multiple regression equations"(Hair et al., 2011). SEM is accepted as a combination of interdependence and dependence techniques with the ability to (i) estimating multiple and interrelated dependence relationships, (ii)representing unobserved concepts present in the relationships, and (iii) define a model for explaining the integral set of relationships.

6.4.2. Testing of theoretical models

The structural model is theoretically represented using a set of structural equations and depicted using a visual diagram. While testing the models using two problems are considered. Firstly, the overall and relative model fit, and secondly, the size, direction, and significance of the structural parameter estimates are generally represented with single-headed arrows (Hair et al., 2011). Assessment of structural model fitness is carried out as same as for CFA given in Table 6.2.

6.4.3. Assumptions of Structural Equation Modelling

The Section explains the methodologies in verifying the assumption of multivariate analysis. Identified four assumptions are (i) Normality, (ii) Homoscedasticity, (iii) Linearity, and (iv) Multicollinearity.

Normality

Normality indicates the shape of data distribution for item-by-item metric variables and correspondence to the normal distribution. Normality is assessed based on skewness and kurtosis values. Distribution is nonnormal if the calculated value for skewness and kurtosis exceeds the critical value of +/-2.58 with 0.01 significance level and =/-1.96 with 0.05 significance level. Values falling between the critical values is an indication

of possessing properties of normal distribution. Table 6.28 provides Zkewness and Multivariate Zkurtosis values.

Table 6.28: Zskewness and Multivariate Zkurtosis values – Child Online Safety

Zskewness (C.R)	Multivariate Zkurtosis (C.R)
(-1.205) – (.297)	1.342

Homoscedasticity

Homoscedasticity refers to the dependent variables exhibiting equal variance levels across the range of predictor variables. Box's M test is used to verify the multivariate h with variance levels of more than one metric variable verified across many groups. Box's results for testing multivariate homogeneity are given in Table 6.29.A nonsignificant value with significance greater than 0.05 is indicating that the assumption of homoscedasticity is satisfied.

Table 6.29: Multivariate Test of Homoscedasticity – Child Online Safety

Box's Test	
Box's M	1796.176
F	9.001
df1	165
df2	14344.819
Sig.	.068

Linearity

Linearity is based on correlational measures of association. Correlations are signifying linear associations while nonlinear effects are not represented. Curvilinear regression is used for checking the linearity. Corresponding results are given in Table 6.30. It is observed that curvilinear regression results have significant value in the linear regression equation model, which satisfies linearity.

Table 6.29: Curvilinear Regression – Child Online Safety

Table 6.30: Curvilinear Regression– Child Online Safety

Equation	Model Summary				
	R Square	F	df1	df2	Sig.
Linear	.530	269.163	1	239	.000
Logarithmic	.416	170.500	1	239	.000
Inverse	.284	94.923	1	239	.000

Quadratic	.459	230.238	2	238	.000
Cubic	.483	170.021	3	237	.000
Compound	.432	181.763	1	239	.000
Power	.340	122.859	1	239	.000
S	.232	72.310	1	239	.000
Growth	.432	181.763	1	239	.000
Exponential	.432	181.763	1	239	.000
Logistic	.432	181.763	1	239	.000

Multicollinearity

Multicollinearity is arising where there is a presence of relationship among the independent predictor variables and is estimated from Tolerance level as well as VIF (Variance Inflation Values). VIF values greater than five and tolerance levels less than 0.2 indicate the presence of multicollinearity. Table 6.31 shows VIF values less than 5 for five variables with tolerance levels greater than 0.2

Table 6.31: Multi-collinearity Estimation – Child Online Safety

Model		**Collinearity Statistics**	
		Tolerance (>0.2)	**VIF (<5)**
Child Online Safety	WC	.590	1.694
	CF	.641	1.560
	IS	.865	1.156
	PE	.599	1.670
	IL	.602	1.661

6.5 Child Online Safety Model

Study performed Structural Equation Modeling using IBM SPSS AMOS version 22. The study involves the testing of a model for Child Online Safety based on technical experts. The model is used for testing the relationships between different factors leading to child online safety. Testing of the model for hypotheses and empirical results and interpretations are given in this section.The study established a structural equation model for verifying the different dimensions of Child Online Safety. The model is used for testing the following hypotheses.

- *H1-Establishing Wanted contact is positively related to Child Online Safety*
- *H2-Content Filtering is positively related to Child Online Safety*
- *H3-Identification Systems is positively related to Child Online Safety*

- *H4-Parental Control and Education Awareness is positively related to Child Online Safety*
- *H5-ISP Level efforts is positively related to Child Online Safety*

Summary of variable counts used in the study is summarized in Table 6.32. The overall fit of the structural model for testing hypotheses is good, with a $\chi 2$ value of 389.261having p-value of 0.155, which is greater than the recommended threshold of 0.05, and the CMIN/DF value of 1.075, which is below 5.0. Again the RMSEA(.018) and SRMR(0.053) are less than 0.08. Furthermore, the GFI (.902), AGFI(.902), NFI(.927), IFI(.994), TLI (.994)and CFI (.994)are well above the recommended threshold of 0.90. All these results suggest that the overall fit of the structural model is good.

Table 6.31: Summary of variable Counts

Number of variables in the model:	65
Number of observed variables:	29
Number of unobserved variables:	36
Number of exogenous variables:	35
Number of endogenous variables:	30

Structural Model Validation for Hypothesis H1

Table 6.32 shows that Establishing Wanted Contact is related to Child Online Safety with a standardized regression weight of 0.251. Hence hypothesis H1 is accepted.

Table 6.32: Structural Model Validation -H1

Hypothesis	**Relationship**	**Unstandardized Regression Weight**	**SE**	**Standardized Regression Weight**	**CR**
H1	CS ← WC	.244	.044	.251	5.600***

Structural Model Validation for Hypothesis H2

Table 6.33 shows that Content Filtering is related to Child Online Safety with a standardized regression weight 0.515. Hence hypothesis H2 is accepted.

Table 6.33: Structural Model Validation -H2

Hypothesis	Relationship	Unstandardized Regression Weight	SE	Standardized Regression Weight	CR
H2	CS ← CF	.512	.053	.515	9.669***

Structural Model Validation for Hypothesis H3

Table 6.34 shows that Identification Systems is related to Child Online Safety with a standardized regression weight 0.017. Hence hypothesis H3 is accepted.

Table 6.34: Structural Model Validation -H3

Hypothesis	Relationship	Unstandardized Regression Weight	SE	Standardized Regression Weight	CR
H3	CS ← IS	.016	.030	.017	.583

Structural Model Validation for Hypothesis H4

Table 6.35 shows that Parental Control and Education Awareness are related to Child Online Safety with a standardized regression weight of 0.332. Hence hypothesis H4 is accepted.

Table 6.35: Structural Model Validation -H4

Hypothesis	Relationship	Unstandardized Regression Weight	SE	Standardized Regression Weight	CR
H4	CS ← PE	.356	.049	.332	7.245***

Structural Model Validation for Hypothesis H4

Table 6.36 shows that ISP-level Efforts is related to Child Online Safety with a standardized regression weight of 0.189. Hence hypothesis H5 is accepted.

Table 6.36: Structural Model Validation -H5

Hypothesis	Relationship	Unstandardized Regression Weight	SE	Standardized Regression Weight	CR
H5	CS ← IL	.191	.049	.189	3.888***

The study established a structural model for Child Online Safety. Through hypothesis testing, the model's fitness is good, and all the five hypotheses are accepted. It is proved

that all five dimensions have significant positive relations with Child Online Safety. Figure 6.8 shows the model for Child Online Safety as a result of the study.

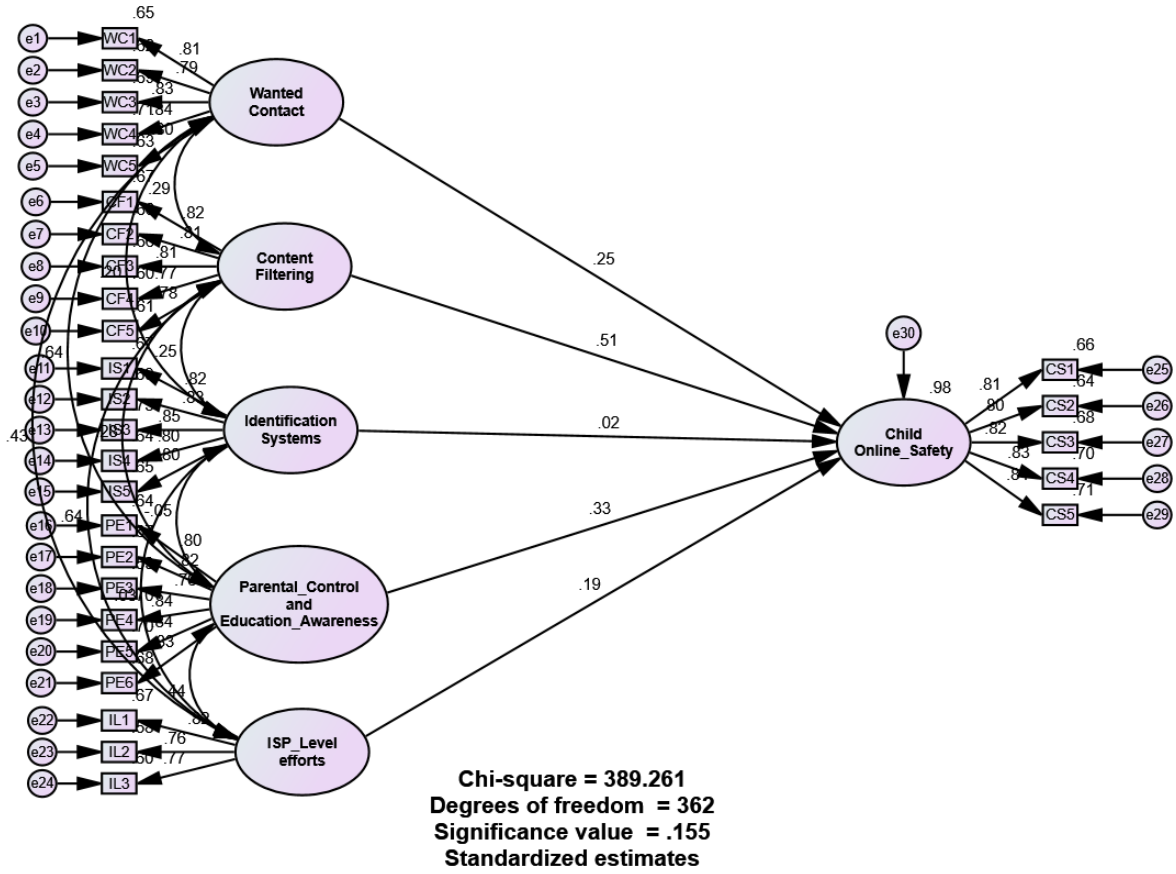

Figure 6.8: Derived Model for Child Online Safety

6.6 Conclusion

The chapter discussed the analysis of primary and detailed interpretation of the results based on the responses from technical experts. The study examined the relationship between Establishing Wanted Contact, Content Filtering, Identification Systems, Parental Control, and Education Awareness and ISP level efforts on Child Online Safety. For this, primary data was collected from technical experts. The study developed a model and tested it using Structural Equation Modeling. Detailed analysis and interpretation were included in the chapter. The study established a generalized model for addressing Child Online Safety. In the next chapter summary of findings, suggestions, and future research directions have been included.

CHAPTER 7

SUMMARY OF FINDINGS, SUGGESTIONS, AND FUTURE RESEARCH

7.1. Introduction

This chapter comprises a summary of findings of the research study, conclusions, and suggestions for improving Child online safety in India. It summarizes the research activity where the summary of the research by revisiting the research questions and objectives and summarizing the limitation of the study. The chapter presents a summary of the empirical study and highlights the findings of the study.

7.2. Summary of Research

Internet is more and more getting a part of life, especially for children and youth. The potential is identified and exploited for communication, including social networking, entertainment, online gaming, and academic activities, including information gathering. Internet is a constant and familiar presence through computing devices, mobile, and other communication technologies. The gap between offline and online is getting reduced day by day, and segregation is becoming meaningless. Global reach, along with anonymous nature, is illegal upbringing activities growing exponentially, targeting children. Online pedophile networks are growing vigorously, and sexual offenders are effectively exploiting the Internet for child exploitation. Convicts are widely using the Internet for disseminating pornographic images, videos, and textual stories in the form of blogs. Additionally, pedophiles use social networking sites, newsgroups, and chat rooms to deceive themselves as children for sexual communication.

As online child safety is a global issue and requires a global response, many countries have taken steps to battle with it by introducing online child safety or protection-related acts and initiated various awareness programs. The preparation of standards and guidelines for children or young people, parents, caretakers, pedagogues, policymakers, and industry is taken up by few international research organizations. From the discussion, the primary focus was made to investigate the developments for the safety of children for protecting them while accessing the content on the Internet. The study focused on research techniques for mitigating online security risks. As stated, the current study emphasizes assessing online child exploitation scenarios and causative factors, risk mitigation frameworks, and internet filtering schemes for online child exploitation avoidance. Hence, a literature survey was carried out with a focus on the approaches used globally, gaps in the approaches, differentiation of the problem, learning from other approaches to the current problem, similar approaches to the other

problems, setting our work into context, avoid wasting efforts and checking for controversial results. Literature survey is identified as one of the methodologies in the entire research period. Based on literature and website survey, classification of online activities leading to online and offline sexual abuse against children was identified, and a review of online grooming and Internet-facilitated sexual exploitation of children was conducted. Based on literature and website surveys, the classification of intermediary vs. direct actors targeting children online was identified. The actors involved in the Internet act as an intermediary and carry out different activities. Activities include content uploading, hosting content, storing content, archiving content, cataloging content, and providing physical access to content. Internet is controlled directly or indirectly by intermediaries, making governments and law enforcement agencies gap in regulating the Internet and cyber-crimes.

Most scholars implement different methods to carry out the research, which depends on the purpose of the research and the type of information required. Both qualitative and quantitative research methods inside any of these rules should be used. The qualitative method has been proposed because it can answer why, how, and in what way. Considering the various filtering techniques and preventive measures of online child exploitation, the empirical study encompasses semi-structured interviews with the different stakeholders to collect responses towards varied factors affecting the successful assessment of opportunities for the stakeholders, and the factors which help in filtering techniques, preventive measures to be taken against online child exploitation such as creating awareness about online child exploitation, proper rules, and guidelines against cyberbullying. Meanwhile, the quantitative approach also has great significance in assessing various key aspects of intended research work and is equally important as qualitative research. Hence, this research intends to employ it where questionnaires and surveys have been used to collect numerical or measurable data from targeted respondents. The researcher's expectations of getting a broader picture of what is expected would also be part of the proposed quantitative research. As already stated, being multi-stakeholder research, here performed analysis for distinctly for various stakeholders.

7.2.1. Problem Statement and Research Question Revisited

Children access online content for educational purposes, and it cannot be denied that the Internet brings lots of opportunities to children. The exploitation of the Internet by children exposes them to new risks and dangers. The exponential rise in internet usage by children for different purposes, including academic, gaming, and social media surfing, has broadened the horizon for intruders or malicious entities to gain a certain point of contact with children that in later stage results in exploitation. Such exploitation can be of different types of forms, such as mental harassment, sexual exploitation, cyber-crimes, and addition towards ill-behaved activities. Online cyber-crime activities might lead to disastrous consequences causing even loss of life and money. Different web-content filtering approaches have been developed; however, their efficacy to avoid cyber-crime mentioned earlier or allied online child exploitation has not yet been studied and verified, at least in the Indian scenario. Different factors can, directly and indirectly, impact the success of any technical approach. Behavioral aspects, perceptual aspects, preferences, and supervision can be there, limiting or promoting the success and failure of online content filtering or parental control to avoid online child exploitation. There can be different perceptions from stakeholders such as children, parents, school teachers or authorities, lawyers and technical experts, children's online search behavior, content filtering, use patterns, and risk assessment. In such diverse conditions, it becomes important to assess the perception of the different stakeholders towards online child behavior, online child exploitation, and allied risks and potential solutions. Realizing these facts as the motive, in this research, the predominant emphasis has been made on assessing the perception of the different stakeholders towards child's online internet surfing behavior, child exploitation risks and alleviating measures, legal issues on content filtering, and probable optimal technical enhancement to prevent online child exploitation using advanced content filtering and multi-channel supervision and coordination systems. To achieve this, in this research, a mixed research paradigm including both qualitative and quantitative methods has been considered. Being an empirical study, responses from different stakeholders, including children, parents, teachers, technical experts, and legal experts, have been examined analytically to understand the root cause of online child exploitation, preventive measures, and a conceptual model alleviate at hand issues.

7.2.2. Research Question Answered

1. How to improve online child safety in the Indian Context

The study is to empirically assessed internet security techniques to safeguard the users and their data from being misused. Different constructs associated for facilitating safe access of online content for children have been examined and provided information the aspects for on protecting children from the harm caused due to cybercrime

7.2.3. Research Objectives Revisited

Escalation in the exploitation of the Internet by people of different age groups has forced the allied authorities and industries to restrict the use of some websites or some user-specific content to confine cybercrime. There are now specially developed numerous techniques to prevent the exploitation of children who visit online websites and provide their details while logging on to any website or using any online platform. The principal goal of this research or study is to assess (empirically) internet security techniques to safeguard the users and their data from being misused. The exploitation of the Internet by children exposes them to new risks and dangers. Hence, this research aims to prevent children from risks encountered while accessing online content since online child exploitation has been a concern across the globe. Children are more prone to face the risks associated with cyber-crime and finally end up harming themselves or their people. In this research, several constructs associated with facilitating safe access of online content for children have been examined, and it has been ensured that the study discusses and provides information about all the aspects allied with mitigation of cyber-crime with a special focus on protecting children from the harm caused due to cybercrime. The current study titled **"Child Online Safety: A Select Study in Indian Context"** emphasizes assessing online child exploitation and causative factors, risk mitigation frameworks, internet filtering schemes for online child exploitation avoidance. The key research objectives of this study are enumerated as follows:

1. To examine the distinctive issues pertinent to online child safety and protection
2. To analyze the adult content identification mechanisms based on E-discovery techniques.
3. To explore the existing global practices addressing Child online safety
4. To study and examine a risk mitigation framework addressing children's online issues in the Indian Context

7.2.4. Justification for the Indian context

Online child safety is a global issue and requires a global response. Countries have taken steps to battle with it by introducing online child safety or protection-related acts and initiated various awareness programs. The preparation of standards and guidelines for children or young people, parents, caretakers, pedagogues, policy makers, and industry is taken up by few international research organizations. When it comes to the growing number of Internet users, especially children, India is not much behind other developed nations. Hence, foreseeing the need for online child safety, the Govt. of India has taken an initiative to formulate a separate sub-section (section 67 B) on online child safety in its Indian IT Act 2000 and Indian IT Act Amendment 2008. National Commission for Protection of Child Rights (NCPCR) has launched the POCSO e-box, enabling the children who are victims of cybercrimes to lodge complaints. Victims are allowed to report cybercrimes through the e-box facility available at the website www.npcr.gov.in. Reporting or complaints can also be made through mobile numbers and email. E-box is identified as a direct channel for reporting under the Protection of Children from Sexual Offences Act, 2012. There is no centralized mechanism in India for the dynamic monitoring of Online child sexual abuse materials (CSAM). The inter-ministerial committee constituted by Ministry of Electronics and Information Technology (MeitY, 2017) deliberated and brought out the issues related to CSAM and methodologies for blocking in India. Depending on the committee Ministry of Electronics and Information Technology recommendation, MeitY has issued an order to Internet Service Providers (ISPs) to adopt and implement Internet Watch Foundation (IWF) resources for preventing online CSAM in India. There is much more left to be done in India to ensure the full safety of teenagers.

7.3. Conceptual Research Model and Explanatory variables revisited

High-speed growth in the functionality of Information and Communication Technologies coupled with high-speed connectivity, wider ranges of services, on-the-fly entries, and exits of mobile has made easy provision for online activities for users across the globe, including children. New technologies set the stage for various types of crimes targeting people across all age groups online and offline based on user practices. It is essential that Internet governance practices have to be made strong, considering children's rights in the digital era. With the rapid growth of the Internet in

India and other developing nations, Internet governance organizations shall shape best practices, including multiple stakeholders, children, parents, teachers, Internet service providers, law enforcement agencies, and governments.

Table 7.1 Explanatory variables – Child Online Safety

Governance	**Technology**	**Societal**
• Security Awareness • Proliferation and controlling • Practises and Guidelines • Grievance Redress • National Framework • Certification Initiatives	• Self-efficacy • Safety Measures • Application Trust • Virtual Harm Exposure • Frequency of Use	• Cultural Characteristics • Individual Characteristics • Parental Mediation • Openness and Coping

The conceptual framework drawn for this confluent mixed method design involves multiple studies depicting the relationship between governance, technology and social factors and children online safety issues. The conceptual framework is derived based on the guidance of theoretical and empirical background previously. Explanatory variables identified for the research are listed in Table 7.1.

7.4. Synthesis of Case Study

The section addresses the synthesis of three case studies in detail: (i) Lab setup providing test results of various commercial and open-source electronic discovery applications;(ii) Analysis of online social media responses and awareness posts on children online safety; (iii) Study on cyberbullying detection in social media text messages.

Synthesis -Adult Content Identification Framework -Test Lab

The technological growth is driving the predators to target the most vulnerable user base, children. Online child safety is identified as a global issue. The promotion of child online safety applications and awareness programs has been initiated internationally.

The case study focused on a survey of various commercial and open-source electronic discovery applications, which shall cater to the identification of age-inappropriate contents in the form of image, text, and video, keywords, documents, and Internet browsing history. The study provides a comparative analysis of common and unique technological features of various solutions. Based on the findings, the research provides an agent-based Client-server framework for adult content identification focusing on child safety.

From the technological perspective for ensuring the safety of children online, two propelling force areas for monitoring and examination have been identified. Firstly, Internet monitoring helps identify sites, determining who transgresses law by disseminating and restricting to adult or explicit content. The second method directs attention to the detection of such contents in computers, information identification about keywords used in Internet searching and filenames, examination of active and deleted files. Both the technological methods require identifying adult content and commonly used keywords in an accurate and faster way. General features for adult content identification applications are identified using the test lab as follows.

- Nudity detection in images and videos
- Keyword scanning and document inspection
- Web browsing history scanning and cookie analysis
- Compressed file scanning, file extension checking, and renamed file identification
- Safe file exclusion, review, and interactive detection of detected offensive materials
- Logotype detection and warning text recognition in adult videos
- Client-Server Architecture

Adult content identification software has various common or unique features or capabilities, including porn detection in images, videos, and audios, file name analysis, web usage history analysis, and many more. Features and capabilities including image analysis, video analysis, keyword search, document analysis, web usage history, file type and name search and enterprise architecture can be considered by the user groups and law enforcement agencies for the effective adult content or porn detection process and ensuring the safety of children while they are online. The feature-wise comparisons

based on an empirical study of well-known adult content identification software are summarized as part of the research.

The present study shows that most of the tools under consideration are not conducting adult content identification from a forensic perspective. Current tools under the analysis are inadequate to identify adult or pornographic content from deleted files, temporary storage of data including clipboard data, recycle bin, and deleted browser history and cookies. Considering the mentioned drawback, the researcher proposes an agent-based Client Server model that Academia can directly implement to monitor student activities. The improved framework consists of an (i) Software Agent installed in an individual host over the network running in the background without any user interface; (ii)Server Software that the network administrator can use to view reports sent by the host machine. Agents are running periodically at specified time intervals depending on the search target, and reports are sent to the server system. Novice features added to adult content detection software, and the architecture of the extended framework are listed below.

- Known content searching using hash database, URL List and Keywords
- Recovery and analysis of deleted internet history
- Periodic capturing of the screenshot and clipboard content
- Host Management, periodic scans, and scan logging

The rapid growth of the Internet has paved the way for the proliferation of multimedia content. Adult content material, including images, videos, audios, and documents, is transmitted over the Internet, exploiting the high-speed connectivity and storage availability. The ease of access, anonymity, and borderless nature of the Internet has made it difficult in curtailing the storage and distribution of adult content. From a technical standpoint, detection of adult content, web browsing history, analysis of documents and files, and Internet monitoring are used to combat issues targeting children online. The study presented a survey of adult content identification solutions and their general characteristics and requirements. Based on the survey of existing tools and solutions, an agent-based Client-Server model was presented. The proposed model provides additional opportunities for effective adult content identification by including analysis of clipboard and screenshot, deleted browser history with an effect is known content search using Hash database, URL list, and keywords from various Child

Internet safety organizations and adult content reporting portals. The framework can be used for effective adult content identification in schools and controlled public places where children use the Internet and computers. The framework proposed by the research can be scaled for deployment in various locations at the national and international level and facilitate the creation of adult content database including URL List, Keywords, Pornographic File Hash list, and Domain alerts which can be used by Law Enforcement Agencies, Government, Non-Governmental Organizations and Academia.

Synthesis -Sentiment Analysis of Social Networking Applications in Indian Context

Children initiate the usage of the Internet at a young age and spend more time online. Apart from the benefits like improved education, entertainment, news, and gaming, the Internet poses severe threats to children online. Providing safety to children in online space is a global challenge. This study aims to examine online social media responses and awareness posts on children's online safety. In this relation, Twitter social media responses after freeing the accusers of children sexual harassment and Facebook pages of some prominent personalities in India for online safety are analyzed. The results reveal that though the people are angry and fearful, they believe judiciary and police system and expecting safety from the same. The analysis of Facebook posts depicts that the concerned authorities are active towards child online safety and awareness through their representatives.

In the first part of the work, the data is collected from the Twitter platform after freeing the accusers of children's sexual harassment in the Southern part of India. The set of incident-related keywords are used to query Twitter social media. As a result of querying, the Twitter media provided a total of 1700 tweets. To know the insights of the Twitter content concerning punishment to the perpetrators of sexual violence, the collected tweets are analyzed in terms of emotions and sentiments. In the second part of the work, the posts related to children's online safety are collected from prominent personalities on Facebook social media. These collected posts are analyzed manually to identify and understand mechanisms adopted to provide children online safety and their impacts. The results are interpreted and recorded accordingly.

In cyberspace, children are vulnerable to threats such as bullying, abuse, sexual abuse, sexting, grooming. The threats to children in the online world may be in the form of

content, usage, and interaction. Though the crimes are taking place, people trust the judiciary and police system by anticipating safety in the future. People expect punishment against the perpetrators of the crime. Several initiatives are taken by governing authorities to combat cybercrimes. The representatives of the concerned units are trying their best to attain online safety for children. The necessary actions should be taken for cybercrime awareness information to reach all social media users. Some of the terms in associated with positive emotions represent the actions against emotions associated with negativity. The popularity level of the posts on social media should be given importance. With the help of these insights, policymakers can design better policies to attain child online safety.

Synthesis -Cyber Bullying detection in Social Media Messages

Cyberbullying has become one of the major problems in social media affecting teenagers. Efficient machine learning algorithms make bullying message detection possible. The researcher used deep learning techniques for Cyberbullying classification based on the bullying content in the message. Convolutional neural networks (CNN) in the area of computer vision and speech recognition are well-known. A new model is proposed, which is a combination of CNN and Long short term memory (LSTM) and constructs a layer of bullying features set on the CNN-LSTM model. The researcher chooses the Twitter dataset and applies pre-processing steps to it. The result is applied to the CNN-LSTM model with a bullying feature set as the first layer researcher focused on two approaches in deep learning (i); CNN-LSTM with max-pool layer and(ii); CNN-LSTM without max-pool layer. The performance analysis of the proposed model is analyzed in terms of accuracy. In the proposed CNN-LSTM without the max-pooling layer, the accuracy is 94.41%. Numerous techniques are surveyed to classify the sentences, which use steps like pre-processing, feature extraction, and classification. Traditional methods and deep learning methods have been compared.

The proposed model consists of only one convolutional layer and has a kernel size 3 and 256 filters. It performs convolution on input data. The activation function is linear rectifier units (ReLU) within the convolutional layer. Only one layer of long short-term memory with the hidden state dimension of 128 filters is used. Epoch is one forward and backward pass of the entire training set. Epochs are varying from 5 to 20 for training. Drop out is a regularization parameter, and it is applied between the

convolutional layer and LSTM layer. Drop out is taken as 0.5. For text classification, it achieved an accuracy of 92%. Cyber-bullying detection based on semantic enhanced marginalized denoising auto-encoder has been described. Initially, researchers constructed a bullying feature layer and taken it as a first layer. Following this layer, a marginalized denoising auto-encoder is used. It stacks several denoising autoencoders, and the result from each layer is concatenated and is taken as a learned representation. The performance analysis of the proposed model is analyzed by estimation of accuracy. The method does not contain the bullying feature set layer. Both the methods CNN-LSTM with max-pool layer and without max-pool layer are compared. The maximum accuracy achieved is 91.67% while using CNN-LSTM without the max-pool layer. The max-pool layer reduces the feature map by reducing the dimensionality, which will increase the efficiency.

A model using a convolutional neural network and long short-term memory is proposed. This model contains a bullying feature set as the first layer, followed by the convolution layer and LSTM layer. The proposed model is compared with the existing CNN-LSTM model for bullying text classification. Compared with the existing machine learning models, the proposed approach has shown better performance with CNN-LSTM without the max-pool layer.

7.5. Synthesis -Quantitative Analysis

Being multi-stakeholder research, research provides the analysis for each stakeholder - Children, Parents, Technical experts, and Legal experts. The analysis is performed distinctly in terms of demographic as well as descriptive components. Based on these identified variables, the different hypotheses on prediction of parent and technical experts-initiated child online safety have been set. A predictive analysis of parents' and technical experts' opinions is performed to test some hypotheses.

Considering the exponentially up-surging rate of online child exploitation and harassment in the last few years, identifying certain inclusive preventive measures is of utmost significance. Understanding root causes, behavioral patterns, preferences and flexibilities, technical possibilities, and legal constraints can enable making an optimal and robust preventive measure to avoid online child exploitation in any form. These facts can be stated as the prime driving force and allied objective behind this empirical study. The principal goal of this research is to assess the perception of the different

stakeholders, including children, teachers, parents, technical and legal experts, to understand root causes, behavioral perception, and possible solutions to avoid online cybercrime and (online) child exploitation. In addition, this research also intends to assess the efficacy of the different web-content filtering, risk-mitigation measures, and parental control paradigm to prevent online child exploitation cases in India.

Implications of the study

As the study identified the determinants of contributors to child online safety, there are some implications of the outcome.

Practical implications: From the study, the variables restricting resources, parental control, and blocking at different levels are observed as important to attain child online safety. The resources required to connect online can be reduced/restricted to the children for their online safety. Parents can control children's activities by monitoring their activities, keeping log records, and denying permission to download unwanted software. From the observation, the other way to attain online child safety is blocking at different levels. It can be attained by blocking suspicious information/applications on mobile devices to blocking at ISP sites. All these identified influencers of online child safety can be used practically to mitigate online threats.

Social implications: Children are the future wealth of the country. Therefore, shaping their future with a healthy environment is essential. In this digitized era, the online platform is also a part of the children's development environment. It demands a better Internet for children. If the safety measures are implemented by considering the observed influencers, such as restricting resources, parental control, and blocking at different levels, there may be reduced online threats. The reduction of online threats results in social harmony by attaining the online safety of the children.

7.6. Design of model for Child Online Safety

The study included the analysis of primary data and detailed interpretation of the results collected from technical experts. Technology experts are expected to suggest different measures to prevent online cybercrimes and exploitation of or on children. Responses can help identify robust filtering or blocking concepts, content filtering and verification before content access, role of Internet Service Providers, effective parental control mechanisms, and education requirements. A total of 287 respondents have been considered for primary data collection, and 241 responses have been identified as valid.

Total six variables are identified for the analysis of Technical Experts as stakeholders in addressing Child Online Security issues. The study analyses the relationship between Wanted Contact (WC), Content Filtering (CF), Identification Systems (IS), Parental control & Education awareness (PE), and ISP Level efforts (IL) with Child Online Safety(CS). The study developed a model for Child Online Safety and was tested using Structural Equation Modelling (SEM).

7.7. Research Synthesis and Deriving a Model Internet Governance Framework in Indian Context

After analyzing the results from multiple methods, integration of results is essential for appropriate decisions. Therefore, in this chapter, an effort is made to combine the results of various studies. Synthesis is an evaluation process to obtain collective information from different studies. Synthesis generalizes the research by integrating empirical researches. Synthesis deals with a review and summarization of the concerned study. To overcome the limited breadth of a single study, synthesis is drawn from multiple studies to cover a wider concept. From the literature review, the different variables related to online child safety are identified. Initially, the variables are identified and categorized broadly as governance, legal and social. Later independent variables such as digital awareness, known contacts, limited online convenience, online benefits, restricting resources, educating on online risks, empowering authorities, parental control, known contacts, content filtering, blocking at different levels, education on online behavior, identification systems and ISP level efforts are identified. Considering the inevitable significance of online child exploitation events in the present day scenario, in this research or study mixed research paradigm was applied to understand internet use patterns amongst children, causes of online child exploitation, risk mitigation measures available, and their respective efficiency, scops for the further possibilities to design an inclusive and robust approach to avoid online child exploitation. Being mixed research paradigm, we applied both qualitative and quantitative methods, which employed secondary and primary data sources, respectively. We considered four primary data sources, including children, parents, technical experts, and legal experts. To obtain the responses, we employed semi-structured interviews to assess respective perceptions and suggestions. Considering the generalization of the research outcome, respondents with different demographics were

considered. The empirical analysis performed in this study found that though the majority of the children state their perception affirmative towards internet usages; however, they did not deny getting addiction that forces them to spend more time on the Internet and socialization on social sites. It eventually was found to be the root causes for getting in contact with malicious users.

On the other hand, pornography and objectionable content access and affinity were also observed to be the prime root causes of children to contact malicious or harassing elements. Even parents too confessed that academic purposes being the dominant purpose makes them provide internet connectivity; though children might contact objectionable contents and eventual harassers despite monitoring. They also recommended developing certain information exchange measures and content filtering approaches to avoid online child exploitation. One more interesting fact surfaced in this study that though parents are aware of social sites, they remain unknown from whom the children contact and connect over social sites and what communication they make. Though parents ensure that the child remains away from Internet-enabled computers and mobile, they spend a short but significant time over the Internet, even not under the shadow of parents or guardians. It gives scope for them to surf different web pages or content, leading towards problematic consequences. Avoiding force recommendation and cookies prevention too can help to avoid unauthorized access of multimedia and search history. It can greatly help to avoid misleading contents to prevent child exploitation. Though, it can be effective only with better cyber counseling. Noticeably, it has been found that a significant fraction of parents confess that their child had confessed about the mischievous online act, harassment, financial loss, physical and physical exploitation. However, the fraction of children confessing about their exploitation is less. In such cases, understanding and monitoring children's behave overtime period is a must. In addition, cyber counseling can also be inculcated to avoid any disadvantages. Access monitoring and content filtering provision can also be vital. The study also revealed that though in major the background or demographics of the children do not have a relation with exploitation, surfing behavior, content access, content sharing, and connectivity are the prime reason causing child exploitation on the Internet. Hence, avoiding such mal-practices might reduce the probability of online child exploitation. This study has revealed that though use patterns and reasons behind

internet usages have minute distinguishing lines, monitoring and controlling content access can be vital as a preliminary effort to avoid online child exploitation. In addition, this study observed that content-centric or specific data access, data sharing, and inter-channel information exchange could be of utmost significance to avoid online child exploitation; however, it requires optimal coordination and understanding between children, parents, and teachers. This study also observed that the malicious users or harassers intend to exploit only those who share their details or contact number or email by registering at certain websites or by stalking the children's activities over social media and their content access types. Avoiding video communication and data sharing can also keep such malicious entities away.

Additionally, this study found that apart from content filtering and parental control, access-log exchange, data access sharing, and inter-channel coordination amongst the different stakeholders such as internet service providers, web applications, and administration can be of utmost significance. However, retaining a common consensus would be the biggest hurdle in achieving the same. The inferences contributed in this study can be vital for the allied stakeholders making or inculcating optimal preventive measures for constructive internet usages in children.

This study integrates the results from literature review, international efforts, case study results, and qualitative analysis and proposes a Child Online Safety framework in India as given in Figure 7.1.

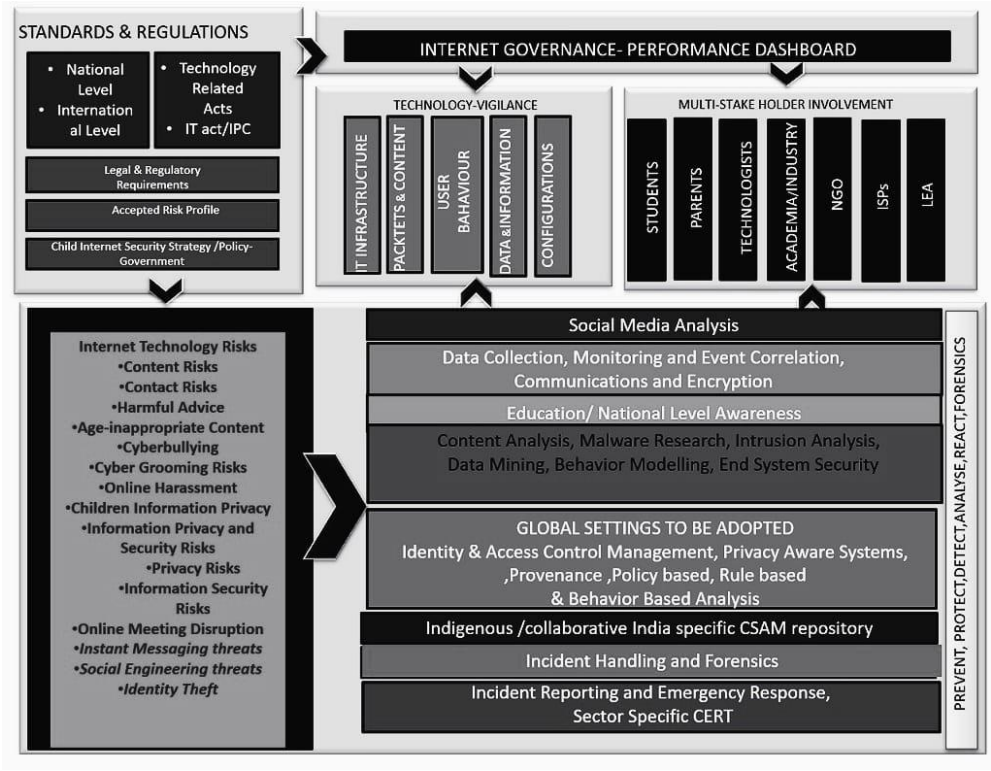

Figure 7.1: Proposed Child Online Safety Framework- India

7.8. Limitations of the Study

The thesis may suffer from limitations. Following are some of the limitations observed in this thesis.

- Tools considered for the case study are not conducting adult content identification from a forensic perspective.
- Tools specifically categorized as parental control software was not used specifically for the research.
- The current study using Sentiment Analysis is limited to Twitter and Facebook social media platforms.
- The tweets are collected and analyzed concerning a single incident.
- There might be chances of missing out on relevant messages or tweets.
- Case study based on Cyberbullying detection in social media text messages has not considered Indian Languages.
- Quantitative analysis is made with the responses collected from only parents and technical experts associated with child online safety initiatives.

- Responses collected from technical experts were only considered in developing the model.
- Even though actions have been taken to reduce the bias imposed by the researcher, knowledge, background, and experience of the researcher may have influenced the research processes, including the selection of the sample, conducting interviews, and data analysis.
- The study has not considered the existing pandemic and social changes while preparing the surveys for children and parents.

7.9. Future Research Directions

The previous sections have discussed the contribution to the thesis and also specifies the limitations of the thesis. This section, therefore, provides future research opportunities that can be undertaken:

- Case study for adult content identification can be extended for tools with forensics capability
- Information posts are analyzed for Sentiment analysis from a few personalities' pages. In the future, the analysis can be extended to other social media, the tweets collected on multiple incidents, and information posts from more pages.
- Cyberbullying detection from Social media text messages can be extended for Indian languages.
- Models may be developed further by using responses from legal professionals and Law Enforcement Agencies.
- The role of existing Computer Emergency Response Teams in Internet Governance can be studied.
- Methodologies for developing indigenous CSAM repositories and OSINT methodologies for addressing online child safety can be explored.
- Research may be further extended in the context of the Covid 19 pandemic and online education platform proliferation.

7.10. Conclusions

This study aims to address the challenges in addressing Child Online Safety issues in the Indian context. The study employed the use of qualitative and quantitative study approaches for examining the various research objectives. The mixed methodology

approach enabled the triangulation of various study findings for comparing and validating the result towards the overall conceptual framework for Child Online Safety in the Indian context. This chapter summarizes the major findings revisiting the research questions, significant study contribution, and study limitations. Suggestions for future work have been included to closing the existing limitations and make the research domain better.

R E F E R E N C E S

Aarambh India. (2014). Why we do what we do. http://aarambhindia.org/about/#y-aarambh. (20 May 2019).

Aboujaoude, E., Savage, M. W., Starcevic, V., &Salame, W. O. (2015). Cyberbullying: Review of an old problem gone viral. *Journal of adolescent health*, *57*(1), 10-18.

ACMA. (2009). Developments in Internet Filtering Technologies and Other Measures forPromotingOnlineSafety.www.acma.gov.au/~/media/Research%20and%20Analysis/Information/pdf/developments_in_Internet_filters_2ndreport%20pdf.pdf (Aug. 15, 2019).

ACMA. (2016). Australian Communication and Media Agency.http://acma.gov.au/ (Aug. 15, 2019).

AIFS. (2015). Images of Children and Young people Online CFCA Resource Sheet. aifs.gov.au/cfca/publications/images-children-and-young-people-online (Feb. 19, 2019).

Aiken, M., Moran, M., & Berry, M. J. (2011, September). Child abuse material and the Internet: Cyberpsychology of online child related sex offending. In *29th meeting of the INTERPOL Specialist Group on Crimes against Children, Lyons, France, September* (pp. 5-7).

Ali,Acılar. (2011). Exploring the aspects of digital divide in a developing country. *Issues in Informing Science and Information Technology*, *8*, 231-244.

All-Party Parliamentary Group for Runaway and Missing Children and Adults (2016) Inquiry into the safeguarding of 'absent' children 'It is good when someone cares' London: The Children's Society/Missing People.

Ally, M., Robinson, M., &Samaka, M. (2016). Initiatives to innovate education to prepare Qatar for the future. In *Transforming Education in the Gulf Region* (pp. 138-153). Routledge.

Allyson, M. M. (2012). Reporting Abuse of Vulnerable Citizens. mcandrewslaw.com/publications-and-presentations/articles/reporting-abuse-of-vulnerable-citizens/ (Feb. 20, 2019).

Anja, B, & Lomborg, S. (2013). Mapping actor roles in social media: Different perspectives on value creation in theories of user participation. *New media & society*, *15*(5), 765-781.

Andrews, Dittin, Sreejith Alathur, and Naganna Chetty. "International efforts for children online safety: A survey." *International Journal of Web Based Communities* 16.2 (2020): 123-133.

Andrews, Dittin, Alathur, S., & Chetty, N. (2020, December). Child Online Safety Intervention Through Empowering Parents and Technical Experts: Indian Context. In *International Working Conference on Transfer and Diffusion of IT* (pp. 662-673). Springer, Cham.

AMF. (2016).Alanahh and Madeline Foundation. https://www.amf.org.au/who-we-are/about-us/. (Jan. 15, 2019).

Attri, R., Dev, N., & Sharma, V. (2013). Interpretive structural modelling (ISM) approach: an overview. *Research Journal of Management Sciences*, *2319*(2), 1171.

Bäckstrand, K. (2006). Multi-stakeholder partnerships for sustainable development: rethinking legitimacy, accountability and effectiveness. *European environment*, *16*(5), 290-306.

Bagozzi, R. P., Yi, Y., & Phillips, L. W. (1991). Assessing construct validity in organizational research. *Administrative science quarterly*, 421-458.

Baltazar, J., Costoya, J., & Flores, R. (2009). The real face of koobface: The largest web 2.0 botnet explained. *Trend Micro Research*, *5*(9), 10.

Barnardo's, I. (2012). Cutting them free: How is the UK progressing in protecting its children from sexual exploitation?.

Barth, J., Bermetz, L., Heim, E., Trelle, S., & Tonia, T. (2013). The current prevalence of child sexual abuse worldwide: a systematic review and meta-analysis. *International journal of public health*, *58*(3), 469-483.

BBC. (2017). Online safety: Internet 'not designed for children' - BBC News. [online] BBC News. http://www.bbc.co.uk/news/education-38508888 (Jan. 26, 201)

Beckett, H., Brodie, I., Factor, F., Melrose, M., Pearce, J. J., Pitts, J., ... & Warrington, C. (2013). *" It's wrong-but you get used to it": a qualitative study of gang-associated sexual violence towards, and exploitation of, young people in England*. University of Bedfordshire.

Beck, U., Lash, S., & Wynne, B. (1992). *Risk society: Towards a new modernity* (Vol. 17). sage.

Behrenshausen, B. G. (2013). The active audience, again: Player-centric game studies and the problem of binarism. *New Media & Society*, *15*(6), 872-889.

Bechmann, A., & Lomborg, S. (2013). Mapping actor roles in social media: Different perspectives on value creation in theories of user participation. *New media & society*, *15*(5), 765-781.

Belanger, F. (2012). Theorizing in information systems research using focus groups. *Australasian Journal of Information Systems*, *17*(2).

Bentler, P. M., &Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological bulletin*, *88*(3), 588.

Berelowitz, S. (2013). If only someone had listened: Office of the Children's Commissioner's inquiry into child sexual exploitation in gangs and groups. Final report.

Berelowitz, S., Firmin, C., Edwards, G., &Gulyurtlu, S. (2012). I thought I was the only one. The only one in the world. *The Office of the Children's Commissioner's Inquiry into Child Sexual Exploitation In Gangs and Groups: Interim report. London: The Office of the Children's Commissioner in England*.

Berelowitz, S., Ritchie, G., & Edwards, G. (2014). "If it's not better, it's not the end": Inquiry into Child Sexual Exploitation in Gangs and Groups: one year on.

Berson, I. R. (2003). Grooming cybervictims: The psychosocial effects of online exploitation for youth. *Journal of School Violence*, *2*(1), 5-18.

BIK Team. (2019). Building a sustainable digital future with the European Safer InternetCentres.https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=4558171(May 25, 2019.

Bilge, L., Strufe, T., Balzarotti, D., &Kirda, E. (2009, April). All your contacts are belong to us: automated identity theft attacks on social networks. In *Proceedings of the 18th international conference on World wide web* (pp. 551-560).

Boshmaf, Y., Muslukhov, I., Beznosov, K., &Ripeanu, M. (2011, December). The socialbot network: when bots socialize for fame and money. In *Proceedings of the 27th annual computer security applications conference* (pp. 93-102).

Bossey, C. de (2005). Report of the Working Group on Internet Governance. http://www.wgig.org/docs/WGIGREPORT.pdf (Jan. 21, 2019).

Brennan, M., Perkins, D. E., Merdian, H. L., Tyrrell, E., Babchishin, K. M., McCartan, K. F., & Kelly, R. (2019). Best practice in the management of online sex offending.

Brown, C. S. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9*(1), 55.

Brown, S., Brady, G., Franklin, A., Bradley, L., Kerrigan, N., & Sealey, C. (2016). Child sexual abuse and exploitation: Understanding risk and vulnerability.

Burnay, J., Billieux, J., Blairy, S., &Larøi, F. (2015). Which psychological factors influence Internet addiction? Evidence through an integrative model. *Computers in Human Behavior*, *43*, 28-34.

Byron, T. (2008). "Safer Children in a Digital World: The Report of the Byron Review". London: Department for Children, Schools and Families, and the Department for Culture, Media and Sport. www.dcsf.gov.uk/ukccis/userfiles/file/FinalReportBookmarked.pdf (Apr. 23, 2019).

Byrne, J., & Burton, P. (2017). Children as Internet users: how can evidence better inform policy debate?. *Journal of Cyber Policy*, *2*(1), 39-52.

Cavanaugh, C., Gillan, K. J., Kromrey, J., Hess, M., &Blomeyer, R. (2004). The effects of distance education on k-12 student outcomes: A meta-analysis. *Learning Point Associates/North Central Regional Educational Laboratory (NCREL)*.

CDAC. (2016). Centre for Development of Advanced Computing. www.cdac.in. (Jan. 20, 2019).

CDT. (2012). Shielding the Messengers: Protecting Platforms for Expression and Innovation.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf (Apr. 30, 2019).

Chakravorty. P. (2016). Key principles of effective prevention education London: PSHE Association.

Child Exploitation and Protection Centre(2011). Scoping Report on Missing and Abducted Children. *London, CEOP*.

CEOP.(2013).Threat Assessment of Child Sexual Exploitation and Abuse. ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf (Feb. 21, 2019).

Childnet. (2016). Childnet International. https://www.childnet.com/. (Jan. 30, 2019).

Children's Commissioner for England. (2016). Protecting children from harm: a critical assessment of child sexual abuse in the family network in England and priorities for action. London: Children's Commissioner for England.

Children's Online Privacy Working Group. (2009). "There ought to be a law: Protecting Children's Online Privacy in the 21st century". A discussion paper for Canadians by the Working Group of Canadian Privacy Commissioners and Child and Youth Advocacies. 19 November. www.ombudsman.yk.ca/pdf/Children'sOnlinePrivacy-e.pdf (Apr. 25, 2019).

Childwise. (2017). Monitor report 2017: Children's media use and purchasing.

Chou, C. M. (2014). Social media characteristics, customer relationship and brand equity. *Journal of Applied Business and Economics*, *16*(1), 128-139.

Cockbain, E., Brayley, H., & Ashby, M. (2014). Not just a girl thing: A large-scale comparison of male and female users of child sexual exploitation services in the UK. *University College London: London, UK*.

Cohen-Almagor, R. (2013). Online child sex offenders: Challenges and counter-measures. *The Howard Journal of Criminal Justice*, *52*(2), 190-215.

Collin, P., Rahilly, K., Richardson, I., & Third, A. (2011). The benefits of social networking services .http://www.fya.org.au/wp-content/uploads/2010/07/The-Benefits-of-Social-Networking-Services.pdf (Feb. 10,2020).

Collings, S. J. (2020). Defining and delimiting grooming in child sexual exploitation. *Child abuse research in South Africa*, *21*(1), 1-9.

Connectsafely. (2016). ConnectSafely organization. www.connectsafely.org/about-us/(<ar. 12 , 2019).

Coomber, R. (1997). Using the Internet for Survey Research'Sociological Research Online, vol. 2, no. 2.c

Cosgrove, M. (2009), "Young French bloggers find a new and risky way to create buzz". Available at www.digitaljournal.com/article/278496 (Sep.30, 2019).

Council of Europe. (2008c). Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet (Adopted by the Committee of Ministers on 20 February 2008 at the 1018th meeting of the Ministers'Deputies). https://wcd.coe.int/ViewDoc.jsp?id=1252427&Site=CM (D=Feb. 21, 2019).

Coy, M. (2009). 'Moved around like bags of rubbish nobody wants': how multiple placement moves can make young women vulnerable to sexual exploitation. *Child Abuse Review: Journal of the British Association for the Study and Prevention of Child Abuse and Neglect*, *18*(4), 254-266.

Coy, M. (2016). Joining the dots on sexual exploitation of children and women: A way forward for UK policy responses. *Critical social policy*, *36*(4), 572-591.

Coy, M. A. D. D. Y. (2016). We don't get this at school: The Safe Choices Reaching Communities Project final evaluation report.

Coy, M., Kelly, L., Elvines, F., Garner, M., &Kanyeredzi, A. (2013). Sex without consent, I suppose that is rape": How young people in England understand sexual consent. *Office of the Children's Commissioner*.

Coy, M., Sharp-Jeffs, N., & Kelly, L. (2017). Key messages from research on child sexual exploitation.

Creswell, J. W. (1994). Research design.

Croll, J. (2016). Let's play it safe: Children and youth in the digital world. ICT Coalition.www.ictcoalition.eu/gallery/100/REPORT_WEB.pdf*(Dec. 21, 2019)*

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *computers & security*, *32*, 90-101.

Dadvar, M., Jong, F. D., Ordelman, R., &Trieschnigg, D. (2012). Improved cyberbullying detection using gender information. In *Proceedings of the Twelfth Dutch-Belgian Information Retrieval Workshop (DIR 2012)*. University of Ghent.

Dadvar, M., Trieschnigg, D., Ordelman, R., & de Jong, F. (2013, March). Improving cyberbullying detection with user context. In *European Conference on Information Retrieval* (pp. 693-696). Springer, Berlin, Heidelberg.

Daramola, D. (2015). Young children as internet users and parents perspectives. *University of Oulu Department of Information Processing Science Master's Thesis, Finland*.

Davidson, J., DeMarco, J., Bifulco, A., Bogaerts, S., Caretti, V., Aiken, M., ... &Puccia, A. (2017). Enhancing police and industry practice: EU child online safety project.

Deb, Sou. (2018). Legislative and Social Measures for Prevention of Child Abuse and Neglect. *An Empirical Investigation into Child Abuse and Neglect in India*, 41-59.

De Haan, J., & Livingstone, S. (2009). Policy and research recommendations. LSE, London: EU Kids Online (Deliverable D5).

DeMarco, J., Sharrock, S., Crowther, T., & Barnard, M. (2018). Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation. *London: Independent Inquiry into Child Sexual Abuse*.

DeNardis, L., & Raymond, M. (2013, November). Thinking clearly about multistakeholder internet governance. In *GigaNet: Global Internet Governance Academic Network, Annual Symposium*.

Denzin, N. K. (1999). Cybertalk and the method of instances. *Doing Internet research: Critical issues and methods for examining the Net*, 107-125.

Department for Education. (2017). Definition and a guide for practitioners, local leaders and decision makers working to protect children from child sexual exploitation London: Department for Education.

DfE (Department for Education) (2014). Preventing and tackling bullying: Advice for headteachers, staff and governing bodies. Retrieved from www.gov.uk/government/uploads/system/uploads/attachment_data/file/444862/Preventing_and_tackling_bullying_advice.pdf.(Dec., 5,2019).

Digital India national flagship programme of the Government of India. https://www.itu.int/en/ITU-D/Regional Presence/AsiaPacific/Documents/Events/2017/Sep-SCEG2017/SESSION-2_India_Mr_Uttam_Chand_Meena.pdf. (Jan., 30, 2020).

Dinakar, K., Reichart, R., & Lieberman, H. (2011, July). Modeling the detection of textual cyberbullying. In *fifth international AAAI conference on weblogs and social media*.

Dinh, T., Farrugia, L., O'Neill, B., Vandoninck, S., &Velicu, A. (2016). Internet safety helplines: exploratory study first findings.

Dodsworth, J, Larsson, B. (2014). An examination of the perspectives and experiences of police officers working with children and young people at risk of, or involved in, child sexual exploitation Norwich: Centre for Research on Children and Families, University of East Anglia.

Dombrowski, S. C., Gischlar, K. L., & Durst, T. (2007). Safeguarding young people from cyber pornography and cyber sexual predation: A major dilemma of the Internet. *Child Abuse Review: Journal of the British Association for the Study and Prevention of Child Abuse and Neglect, 16*(3), 153-170.

Dooley, J. J., Cross, D., Hearn, L., &Treyvaud, R. (2009). Review of existing Australian and international cyber-safety research.

Dowdell, E. B. (2013). Use of the Internet by parents of middle school students: Internet rules, risky behaviours and online concerns. *Journal of Psychiatric and Mental Health Nursing*, *20*(1), 9-16.

Drew, J. (2016). An independent review of South Yorkshire Police's handling of child sexual exploitation 1997-2016.

Dutta, S.,Bilbao-Osorio, B. (2012). The global information technology report 2012. *WorldEconomicForum*,http://www3.weforum.org/docs/Global_IT_Report_2012.pdf (Apr. 25, 2019).

ECPAT. (2016). ECPAT International. www.ecpat.org (Apr. 10, 2018).

ECPAT International. (2018). Ending the sexual exploitation of children. https://www.ecpat.org/news/annual-report/(Apr. 10, 2019).

Edwards-Groves, C., & Langley, M. (2009). i-Kindy: Responding to home technoliteracies in the kindergarten classroom. *Teacher Education*, *35*(1), 89-103.

Edwards, L. (2010). The role and responsibility of internet intermediaries in the field of copyright and related rights.

Edwards, S., Nolan, A., Henderson, M., Mantilla, A., Plowman, L., &Skouteris, H. (2018). Young children's everyday concepts of the internet: A platform for cyber-safety education in the early years. *British journal of educational technology*, *49*(1), 45-55.

Elishar, A., Fire, M., Kagan, D., &Elovici, Y. (2012, December). Organizational intrusion: Organization mining using socialbots. In *2012 International Conference on Social Informatics* (pp. 7-12). IEEE.

eNacso. (2009). "Developing a Response to a new breed of location services". www.enacso.eu/index.php?option=com_rokdownloads&view=file&task=download&id=8%3Aenacso-response-to-the-new-breed-of-locationservices&Itemid=11(Jan. 11 , 2020).

End Violence Against Women Coalition. (2011). A Different World is Possible: Promising Practices to Prevent Violence Against Women and Girls London: End Violence Against Women Coalition.

ENISA. (2007), "Security Issues and Recommendations for Online Social Networks". ENISA Position Paper No.1. www.enisa.europa.eu/act/res/otherareas/social-

networks/security-issues-and-recommendations-for-online-socialnetworks/ at_download/fullReport (Apr.18, 2018).

EUkids online. (2014). EU Kids Online recent research findings, methods and recommendations.https://lsedesignunit.com/EUKidsOnline/offline/download.pdf(Apr. 25, 2019).

Factor, F., Pitts, J., Bateman, T., & Goodfellow, P. (2015). Gang-involved young people: custody and beyond: a practitioner's guide.

Fielder, A., Gardner, W., Nairn, A., & Pitt, J. (2007). Fair game? Assessing commercial activity on children's favourite websites and online environments. *National Consumer Council of the United Kingdom. http://www. ncc. org. uk/news_press/pr. php*.

Firmin, C. (2011). This is it: This is my life. *Female Voice in Violence Final Report: On the Impact of Serious Youth Violence and Criminal Gangs on Women and Girls across the Country*.

Firmin, C. (2013). Something Old or Something New: Do Pre-Existing Conceptualisations of Abuse Enable a Sufficient Response to Abuse in Young People's Relationships and Peer-Groups?. In *critical perspectives on child sexual exploitation and related trafficking* (pp. 38-51). Palgrave Macmillan, London.

Fox, C. (2016). It's not on the radar. *The hidden diversity of children and young people at risk of sexual exploitation in England. Barnardo's*.

Franklin, A., Raws, P., & Smeaton, E. (2015). *Unprotected, overprotected: Meeting the needs of young people with learning disabilities who experience, or are at risk of, sexual exploitation*. Barnardo's.

FTC. (2002). Protecting Children's Privacy Under COPPA: A Survey on Compliance. https://www.ftc.gov/sites/default/files/documents/rules/children%E2%80%99s-online-privacy-protection-rule-coppa/coppasurvey.pdf, (Feb. 20 2019.

FTC. (2016). Federal Trade Commission.www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule(Mar.20, 2020).

Gay, L. R., Mills, G. E., & Airasian, P. W. (2009). Educational research competencies for analysis and applications. Merrill/Pearson,.

Gencer, S. L., &Koc, M. (2012). Internet abuse among teenagers and its relations to internet usage patterns and demographics. *Journal of Educational Technology & Society*, *15*(2), 25-36.

Ghosh, A. K., Badillo-Urquiola, K., Rosson, M. B., Xu, H., Carroll, J. M., & Wisniewski, P. J. (2018, April). A matter of control or safety? Examining parental use of technical monitoring apps on teens' mobile devices. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1-14).

Giannarou, Lefkothea, and Efthimios Zervas. "Using Delphi technique to build consensus in practice." *International Journal of Business Science & Applied Management (IJBSAM)* 9.2 (2014): 65-82.

Gilligan, P. (2016). Turning it around: What do young women say helps them to move on from child sexual exploitation?. *Child abuse review*, *25*(2), 115-127.g

Gohir, S. (2013). Unheard voices: The sexual exploitation of Asian girls and young women. *Birmingham: Muslim Women's Network UK*.

Gong, Z., & Yu, T. (2010, November). Chinese web text classification system model based on Naive Bayes. In *2010 International Conference on E-Product E-Service and E-Entertainment* (pp. 1-4). IEEE.

Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *International Journal of Law and Information Technology*, *10*(2), 139-223.

Google. (2016). Block Adult Sites on Google at Your School or Workplace, Available at: support.google.com/websearch/answer/186669?hl=en(Jan. 26,2019).

Habibi, A., Sarafrazi, A., &Izadyar, S. (2014). Delphi technique theoretical framework in qualitative research. *The International Journal of Engineering and Science*, *3*(4), 8-13.

Hadžović, S., Šerval, D., &Kovačević, S. (2015, May). Regulatory aspects of child online protection. In *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 409-412). IEEE.

Halder, D., & Jaishankar, K. (2014). Patterns of sexual victimization of children and women in the multipurpose social networking sites. *Social Networking as a Criminal Enterprise*.

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2011). Multivariate data analysis. Vectors , Vol. 6.

Hasebrink, U., Livingstone, S., Haddon, L., &Olafsson, K. (2009). Comparing children's online ohir(Feb. 20, 2019).

Hashish, Y., Bunt, A., & Young, J. E. (2014, April). Involving children in content control: a collaborative and education-oriented content filtering approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1797-1806).

Hassan, A., & Mahmood, A. (2018). Convolutional recurrent deep learning model for sentence classification. *Ieee Access*, *6*, 13949-13957.

Hill, R. (2014). The Internet, its governance, and the multi-stakeholder model. *Info*.

Hinduja, S., &Patchin, J. W. (2007). Offline consequences of online victimization: School violence and delinquency. *Journal of school violence*, *6*(3), 89-112.

Hinduja, S., &Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant behavior*, *29*(2), 129-156.

Hinduja, S., &Patchin, J. W. (2014). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Corwin press.

Hof, S., Van den Berg, B., &Schermer, B. (Eds.). (2014). *Minding minors wandering the web: Regulating online child safety*. TMC Asser Press.

Holloway, D., & Green, L. (2013). Using ethnography to understand everyday media practices in Australian family life. *The international encyclopedia of media studies*, 365-386.

Holloway, D., Green, L., & Livingstone, S. (2013). Zero to eight: Young children and their internet use.

Hooper, D., Coughlan, J., & Mullen, M. R. (1831). Structural equation modelling: Guidelines for determining model fit Electron. *J. Bus. Res. Methods*, *6*(1), 1822.

Hopkins, L., Brookes, F., & Green, J. (2013). Books, bytes and brains: The implications of new knowledge for children's early literacy learning. *Australasian Journal of early childhood*, *38*(1), 23-28.

Freedom House. (2009). Freedom on the net: A global assessment of internet and digital media. *Washington, DC: Freedom House*.

Hubbard, A., & Bygrave, L. A. (2009). Internet Governance Goes Global.

IAMAI.(2015). Eleventh Annual report 2014- 15. www.iamai.in/sites/default/files/annual_report/AnnualReport2014-15.pdf (Feb. 19, 2019).

Indian IT Act. (2000). Available at:www.dot.gov.in/sites/default/files/itbill2000_0.pdf (Apr.30,2019).

INHOPE. (2016). INHOPE Association. www.inhope.org/gns/home.aspx (Mar. 20, 2019).

Internet world stats.com. (2021). World Internet Stats. Usage and population statistics, from http://www.Internetworldstats.com/stats.htm(Apr. 10, 2021).

Internet Safety Technical Task Force. (2008). Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States. cyber.harvard.edu/pubrelease/isttf/ (Feb. 10, 2020).

Isaac, D., Cusimano, M. D., Sherman, A., & Chipman, M. (2004). Child safety education and the world wide web: an evaluation of the content and quality of online resources. *Injury Prevention*, *10*(1), 59-61

ISEA. (2014). Indulge with Information Security Education and Awareness. 00_Indulge.pdf (infosecawareness.in) (Feb. 19, 2019).

ISOC. (2013). Internet Society Questionnaire on Multistakeholder Governance. Report and Summary. http://www.internetsociety.org/doc/internet-society-questionnaire-multistakeholder-governance-report-and-summary-results-octobe(Mar.19, 2020).

ISTTF. (2008). Internet safety technical task force. https://cyber.harvard.edu/research/isttf (Feb.21, 2019).

ITU. (2009). Guidelines for Policy Makers on Child Online Protection. www.itu.int/en/cop/Documents/guidelines-policy%20makers-e.pdf(Feb. 19, 2019).

ITU. (2009a), Guidelines for Policy Makers of Child Online Protection. www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/policy_makers.pdf (Jan. 6, 2018)

ITU. (2009b), Tokyo Communiqué on Safer Internet Environment for Children as agreed by participants to the ITU/ MIC Strategic Dialogue on “Safer Internet Environment for Children” on 3 June 2009 in Tokyo, Japan. www.itu.int/osg/csd/cybersecurity/gca/cop/meetings/june-tokyo/documents/ITU-okyo-Communique.doc (Feb. 19, 2019).

ITU. (2015). Child Online Protection Initiative, www.itu.int/en/cop/Pages/default.aspx (Mar. 20, 2019).

Ivaturi, K., & Chua, C. (2019). Framing norms in online communities. *Information & Management*, *56*(1), 15-27.

IWF. (2013). Internet watch foundation annual & charity report 2013. https://www.iwf.org.uk/sites/default/files/reports/2016-03/ar_final_web_low%20res.pdf, (Jan. 21, 2019).

IWF. (2016). Internet Watch Foundation.www.iwf.org.uk(Apr. 20, 2020)

Jackson, L. A., Von Eye, A., Biocca, F. A., Barbatsis, G., Zhao, Y., & Fitzgerald, H. E. (2006). Does home internet use influence the academic performance of low-income children?. *Developmental psychology*, *42*(3), 429.

Jago, S., Arocha, L., Brodie, I., Melrose, M., Pearce, J. J., & Warrington, C. (2011). *What's going on to safeguard children and young people from sexual exploitation? how local partnerships respond to child sexual exploitation*. University of Bedfordshire.

Johnson, D. E., Oles, F. J., Zhang, T., & Goetz, T. (2002). A decision-tree-based symbolic rule induction system for text categorization. *IBM Systems Journal*, *41*(3), 428-437.

Johnson, G. M. (2010). Young children's Internet use at home and school: Patterns and profiles. *Journal of Early Childhood Research*, *8*(3), 282-293.

Johnson, M., Bledsoe, C., Pilgrim, J., & Lowery-Moore, H. (2019). Twitter: A Tool for Communities of Practice. *SRATE Journal*, *28*(1).

Jones, R. S., Zahl, A., & Huws, J. C. (2001). First-hand accounts of emotional experiences in autism: A qualitative analysis. *Disability & Society*, *16*(3), 393-401.

Jones, S., Millermaier, S., Goya-Martinez, M., & Schuler, J. (2008). Whose space is MySpace? A content analysis of MySpace profiles. *First monday*.

Judge, S., Puckett, K., & Bell, S. M. (2006). Closing the digital divide: Update from the early childhood longitudinal study. *The Journal of Educational Research*, *100*(1), 52-60.

Kaiser Family Foundation. (2006), It's Child's Play: Advergaming and the Online Marketing of Food to Children. www.kff.org/entmedia/upload/7536.pdf (Dec.23, 2019).

Kaplan, D. (2004). The Sage handbook of quantitative methodology for the social sciences. sage.

Kardefelt-Winther, D. (2015). A critical account of DSM-5 criteria for internet gaming disorder. *Addiction Research & Theory*, *23*(2), 93-98.

Katz, A. (2016). *Making Your Secondary School E-safe: Whole School Cyberbullying and E-safety Strategies for Meeting Ofsted Requirements*. Jessica Kingsley Publishers.

Kaye, J. J. (2011, May). Self-reported password sharing strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 2619-2622).

Kerlinger, F. N. (1973). Review of research in education.

Kim, K. K., Lee, A. R., & Lee, U. K. (2019). Impact of anonymity on roles of personal and group identities in online communities. *Information & Management*, *56*(1), 109-121.

Kitzinger, J. (1995). Qualitative research: introducing focus groups. *Bmj*, *311*(7000), 299-302.

Klatt, T., Cavner, D., & Egan, V. (2014). Rationalising predictors of child sexual exploitation and sex-trading. *Child Abuse & Neglect*, *38*(2), 252-260.

Kleinwächter, W. (2007). *The Power of Ideas: Internet Governance in a Global Multi Stakeholder Environment*. Marketing für Deutschland.

Klika, J. B., Haboush-Deloye, A., &Linkenbach, J. (2019). Hidden protections: Identifying social norms associated with child abuse, sexual abuse, and neglect. *Child and adolescent social work journal*, *36*(1), 5-14.

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online child sexual exploitation: Prevalence, process, and offender characteristics. *Trauma, Violence, & Abuse*, *15*(2), 126-139.

Kristensen, S. M., & Smith, P. K. (2003). The use of coping strategies by Danish children classed as bullies, victims, bully/victims, and not involved, in response to different (hypothetical) types of bullying. *Scandinavian Journal of Psychology*, *44*(5), 479-488.

Kumar, K., & Pande, B. P. (2021). Rise of Online Teaching and Learning Processes During COVID-19 Pandemic. In *Predictive and Preventive Measures for Covid-19 Pandemic* (pp. 251-271). Springer, Singapore.

Kummer, M. (2012). Children and the Internet. [online] Internet society. https://www.internetsociety.org/sites/default/files/bp-childrenandtheinter (Apr.19, 2020).

Laidlaw, E. (2012). The responsibilities of free speech regulators: An analysis of the Internet Watch Foundation. *International Journal of Law and Information Technology*, *20*(4), 312-345.

Lebloch, E. K., & King, S. (2006). Child sexual exploitation: A partnership response and model intervention. *Child Abuse Review*, *15*.

Lenhart, A., Madden, M., Smith, A., Purcell, K., Zickuhr, K., & Rainie, L. (2011). Teens, Kindness and Cruelty on Social Network Sites: How American Teens Navigate the New World of" Digital Citizenship". *Pew Internet & American Life Project*.www.pewInternet.org/2011/11/09/teens-kindness-and-cruelty-on-social-network-sites/ (Feb. 10,2019)

Lewis, M., Miller, P., &Buchalter, A. R. (2009, October). Internet crimes against children: an Annotated bibliography of major studies. Federal Research Division, Library of Congress.

Livingstone, S. (2013). Online risk, harm and vulnerability: Reflections on the evidence base for child Internet safety policy. *ZER: Journal of Communication Studies*, *18*(35), 13-28.

Livingstone, S., &Bober, M. (2005). UK children go online: Final report of key project findings. http://eprints.lse.ac.uk/399/(Apr.18, 2020).

Livingstone, S., Görzig, A., &Ólafsson, K. (2011). Disadvantaged children and online risk. http://eprints.lse.ac.uk/33730/ (Apr.,21,2019).

Livingstone, S., Davidson, J., Bryce, J., Batool, S., Haughton, C., & Nandi, A. (2017). Children's online activities, risks and safety: a literature review by the UKCCIS evidence group.

Livingstone,S.,&Haddon,L.(2009).EUKidsOnline. *ZeitschriftFürPsychologie/Journal of Psychology*, *217*(4), 236.

Livingstone, S., & Haddon, L. (Eds.). (2012). *Children, risk and safety on the internet: Research and policy challenges in comparative perspective*. Policy Press.

Livingstone, S., Haddon, L., Görzig, A., &Ólafsson, K. (2011). Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries.

Livingstone, S., &Helsper, E. J. (2008). Parental mediation of children's internet use. *Journal of broadcasting & electronic media*, *52*(4), 581-599.

Livingstone, S., Kirwil, L., Ponte, C., &Staksrud, E. (2013). In their own words: what bothers children online? with the EU Kids Online Network.

Livingstone, S., Mascheroni, G., Dreier, M., Chaudron, S., &Lagae, K. (2015). How parents of young children manage digital devices at home: The role of income, education and parental style.

Livingstone, S., Mascheroni, G., &Staksrud, E. (2018). European research on children's internet use: Assessing the past and anticipating the future. *New media & society*, *20*(3), 1103-1122.

Livingstone, S., Ólafsson, K., O'Neill, B., &Donoso, V. (2012). Towards a better internet for children: findings and recommendations from EU Kids Online to inform the CEO coalition. http://eprints.lse.ac.uk/44213/ (Apr., 19, 2020).

Livingstone, S., & O'Neill, B. (2014). Children's rights online: Challenges, dilemmas and emerging directions. In *Minding minors wandering the web: Regulating online child safety* (pp. 19-38). TMC Asser Press, The Hague.

Livingstone, S., & Palmer, T. (2012). Identifying vulnerable children online and what strategies can help them.http://eprints.lse.ac.uk/44222/ (Apr.19, 2020)

Livingstone, S., & Smith, P. K. (2014). Annual research review: Harms experienced by child users of online and mobile technologies: The nature, prevalence and management of sexual and aggressive risks in the digital age. *Journal of child psychology and psychiatry*, *55*(6), 635-654.

Livingstone, S., Stoilova, M., Yu, S. H., Byrne, J., &Kardefelt-Winther, D. (2018). Using mixed methods to research children's online opportunities and risks in a global context: the approach of Global Kids Online.

Macho, S. (2006). *The impact of home internet access on test scores*. Cambria Press.

MacKinnon, R., Hickok, E., Bar, A., & Lim, H. I. (2015). *Fostering freedom online: The role of internet intermediaries*. UNESCO Publishing.

Madigan, S., Villani, V., Azzopardi, C., Laut, D., Smith, T., Temple, J. R., ... &Dimitropoulos, G. (2018). The prevalence of unwanted online sexual exposure and solicitation among youth: a meta-analysis. *Journal of Adolescent Health*, *63*(2), 133-141.

Mantelero, A. (2016). Children online and the future EU data protection framework: empirical evidences and legal analysis. *International Journal of Technology Policy and Law*, *2*(2-4), 169-181.

Marshall, K. (2014). Child Sexual Exploitation in Northern Ireland Report of the Independent Inquiry. *RQIA, Northern Ireland*.

Marsh, J. (2010). Young children's play in online virtual worlds. *Journal of early childhood research*, *8*(1), 23-39.

Martellozzo, E. (2013). *Online child sexual abuse: Grooming, policing and child protection in a multi-media world*. Routledge.

Martin, J., &Alaggia, R. (2013). Sexual abuse images in cyberspace: Expanding the ecology of the child. *Journal of child sexual abuse*, *22*(4), 398-415.

Martin, L., Brady, G., Kwhali, J., Brown, S., &Matouskova, G. (2014). Social workers' knowledge and confidence when working with cases of child sexual abuse: What are the issue and challenges?.

Marwick, A. E., Murgia-Diaz, D., & Palfrey, J. G. (2010). Youth, privacy and reputation (literature review).

McAlinden, A. M. (2012). *'Grooming'and the Sexual Abuse of Children: Institutional, Internet and Familial Dimensions*. Oxford University Press.

McAndrews, A. (2012). Reporting Abuse of Vulnerable Citizens, mcandrewslaw.com/publications-and-presentations/articles/reporting-abuse-of-vulnerable-citizens(Mar. 15, 2019).

McNeish, D., & Scott, S. A. R. A. (2015). An independent evaluation of Rape Crisis Scotland's sexual violence prevention project. *DMSS Research*.

MCIT. (2009). Department of Information Technology Information Technology (Procedure and Safeguards for intercepting, monitoring, and decryption) Rules.www.cca.gov.in/cca/sites/default/files/files/gsr780.pdf (Sep. 19, 2018).

MCIT. (2011). Department of Information Technology Information Technology (Reasonable security practices and procedures and Sensitive personal data or information) Rules. www.wipo.int/edocs/lexdocs/laws/en/in/in098en.pdf(Sep. 19, 2018).

McNally, B., Kumar, P., Hordatt, C., Mauriello, M. L., Naik, S., Norooz, L., ... &Druin, A. (2018, April). Co-designing mobile online safety applications with children. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1-9).

Media Awareness Network (2005), “Young Canadians in a Wired World: Phase II Trends and Recommendations”. www.mediaawareness.ca/english/research/YCWW/phaseII/upload/YCWWII_trends_recomm.pdf (Apr.20,2019).

Melrose, M. (2013). Young people and sexual exploitation: A critical discourse analysis. In *Critical perspectives on child sexual exploitation and related trafficking* (pp. 9-22). Palgrave Macmillan, London.

Menon, J. Why India lags in tackling online child sex abuse.https://timesofindia.indiatimes.com/india/why-india-lags-in-tackling-online-child-sex-abuse/articleshow/74008263.cms, last accessed 2020/02/10.

Michael Chan. (2015). Mobile phones and the good life: Examining the relationships among mobile use, social capital and subjective well-being. *New Media & Society, 17*(1), 96-113.

Mikolov, T., Chen, K., Corrado, G., & Dean, J. (2013). Efficient estimation of word representations in vector space. *arXiv preprint arXiv:1301.3781*.

Millwood, A., & Livingstone, S. (2009). Harm and offence in media content: A review of the empirical literature. *Bristol: Intellect*.

Millwood Hargrave, A. (2009). “Protecting children from harmful content”. Report prepared for the Council of Europe’s Group of Specialists on Human Rights in the InformationSociety.www.coe.int/t/dghl/standardsetting/media/Doc/HInf(2009)13_en.pdf (Fe.20, 2020).

Mishna, F., Saini, M., & Solomon, S. (2009). Ongoing and online: Children and youth's perceptions of cyber bullying. *Children and Youth Services Review, 31*(12), 1222-1228.

Mislove, A., Viswanath, B., Gummadi, K. P., &Druschel, P. (2010, February). You are who you know: inferring user profiles in online social networks. In *Proceedings of the third ACM international conference on Web search and data mining* (pp. 251-260).

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2001). Risk factors for and impact of online sexual solicitation of youth. *Jama, 285*(23), 3011-3014.

Modecki, K. L., Minchin, J., Harbaugh, A. G., Guerra, N. G., &Runions, K. C. (2014). Bullying prevalence across contexts: A meta-analysis measuring cyber and traditional bullying. *Journal of Adolescent Health, 55*(5), 602-611.

Mohanty, A. (2011). New Crimes under the Information Technology (Amendment) Act. *Indian JL & Tech.*, *7*, 103.

Myers, J. and Carmi, E. (2016). The Brooke serious case review into child sexual exploitation: identifying the strengths and gaps in the multi-agency responses to child sexual exploitation in order to learn and improve Bristol: Bristol Safeguarding Children Board.

MySpace. (2008). Joint statement on key principles of social networking sites safety. https://classic.nga.org/files/live/sites/NGA/files/pdf/0809CYBERRESOURCENETWORKING.PDF(Feb .21, 2019).

Nahar, V., Li, X., & Pang, C. (2013). An effective approach for cyberbullying detection. *Communications in information science and management engineering*, *3*(5), 238.

Narayanan, B. K., & Nirmala, M. (2018). Adult content filtering: Restricting minor audience from accessing inappropriate internet content. *Education and Information Technologies*, *23*(6), 2719-2735.

Nawaila, M. B., Kanbul, S., &Ozdamli, F. (2018). A review on the rights of children in the digital age. *Children and Youth Services Review*, *94*, 390-409.

NCMEC. (1998). National Centre for Missing and Exploited Children. http://www.missingkids.org/footer/about/history.(Mar. 19, 2019).

Netnanny. (2019). Net Nanny: Parental Control Software & Website Blocker | Net Nanny (Oct. 5 , 2020).

Netsafe. (2018). Netsafe annual report 2017/2018. https://www.netsafe.org.nz/wp-content/uploads/2018/11/Netsafe-Annual-Report-2018-FinalA1.pdf.(Mar.15, 2018).

NCAB. (2016). National Centre Against Bullying, www.ncab.org.au/who-we-are/about-us/ (Mar. 25,2019).

NCMEC. (2016). National Centre for Missing and Exploited Children.www.missingkids.org/home(Mar. 25,2019).

Netsafe NZ. (2016). Netsafe New Zealand.www.netsafe.org.nz/aboutnetsafe/ (Mar. 25,2019).

NIST. (1998). Information Technology Security Training Requirements: A Role and Performance Based Model, NIST-SP 800-16, USA. csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (Feb. 19, 2019).

Normand, C. L., &Sallafranque-St-Louis, F. (2016). Cybervictimization of young people with an intellectual or developmental disability: Risks specific to sexual solicitation. *Journal of Applied Research in Intellectual Disabilities, 29*(2), 99-110.

Nurrahmi, H., &Nurjanah, D. (2018, March). Indonesian twitter cyberbullying detection using text classification and user credibility. In *2018 International Conference on Information and Communications Technology (ICOIACT)* (pp. 543-548). IEEE.

Nworgu, B. G. (1991). Educational research: Basic issues and methodology. Ibadan. Wisdom Publishers Ltd. NGO clients TOTAL Number Distributed, 3(6), 3.

O'Connell, R. (2003). A typology of child cybers exploitation and online grooming practices. *Cyberspace Research Unit, University of Central Lancashire*.

O'Connor, H., & Madge, C. (2000). Cyber-parents and cyber-research: Exploring the Internet as a medium for research. *Centre for Labour Market Studies, University of Leicester, UK*.

OECD. (2006), "Mobile Commerce". OECD Digital Economy Paper 124, Directorate for Science, Technology and Industry, OECD, Paris. www.oecd.org/dataoecd/22/52/38077227.pdf (Jan. 15, 2019).

OECD. (2007b). Working Party on Regulatory Management and Reform: Methodological Guidance and Frameworks for RIA, GOV/PGC/REG (2007)8.

OECD. (2009a), "Report on the APEC-OECD Joint Symposium on Initiatives among Member Economies Promoting Safer Internet Environment for Children".www.oecd.org/dataoecd/46/46/44120262.pdf (Jan. 15,2019).

OECD.(2009b). Computer Viruses and Other Malicious Software. A Threat to the Internet Economy. OECD, Paris. www.oecd.org/document/16/0,3343,en_2649_34223_42276816_1_1_1_37441,00.html (Jan. 15,2019).

OECD. (2010b). The role of Internet Intermediaries in Advancing Public Policy Objectives. Forging Partnership for Advancing Policy Objectives for the Internet Economy, Part II and III. ICCP(2010)11, OECD, Paris(Jan. 15,2019).

Ofcom. (2014b). Ofcom report on internet safety measures – Internet service providers: Network level filtering measure. www.ofcom.org.uk/__data/assets/pdf_file/0019/27172/Internet-safety-measures-second-report.pdf (Jan. 15,2019).

Ofcom. (2016a). Children and parents: Media use and attitudes report. www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf(Jan. 15,2019).

Ofcom. (2016b). Children's media lives – Year 2 findings. www.ofcom.org.uk/__data/assets/pdf_file/0021/80715/children_media_lives_year2.pdf(Jan. 15,2019).

O'Neill, B. (2014). First Report on the Implementation of the ICT Principles. *Dublin: Dublin Institute of Technology*.

O'Neill, B., Dinh, T. (2018). The Better Internet for Kids Policy Map: Implementing the European Strategy for a Better Internet for Children in European Member States. https://www.betterinternetforkids.eu/documents/167024/2637346/BIK+Map+report+-+Final+-+March+2018/a858ae53-971f-4dce-829c-5a02af9287f7.(Oct. 21, 2019).

Online Safety and Technology Working Group (OSTWG). (2010), "Youth Safety in a Living Internet: Report of the Online Safety and Technology Working Group", 4 June 2010, p. 16. www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf (Aug.19, 2019).

Opinion Leader (2013). Cybersafe: Research to support a safer internet campaign. www.internetmatters.org/wp-content/uploads/2015/12/Cybersafe-20-Sept-2013-Opinion-Leader-FINAL-VERSION-1.pdf.

Opstad, H. (2019). G353 (P) Using the socks teaching programme to increase awareness of online safety/cyberbullying in primary school children. socks: stamp out cyberbullying and keep safe!.

Ost, S. (2009). *Child pornography and sexual grooming: Legal and societal responses*. Cambridge University Press.

Owens, E. W., Behun, R. J., Manning, J. C., & Reid, R. C. (2012). The impact of Internet pornography on adolescents: A review of the research. *Sexual Addiction & Compulsivity*, *19*(1-2), 99-122.

Özel, S. A., Saraç, E., Akdemir, S., & Aksu, H. (2017, October). Detection of cyberbullying on social media messages in Turkish. In *2017 International Conference on Computer Science and Engineering (UBMK)* (pp. 366-370). IEEE.

Palmer, T. (2015). Digital dangers: The impact of technology on the sexual abuse and exploitation of children and young people. *Barnardo's, available online at http://www. barnardos. org. uk/onlineshop/pdf/digital_dangers_report. pdf (Aug. 15, 2019)*

Park, S. (2011). Effects of home environment on Internet use and dependence of children and adolescents. *AoIR Selected Papers of Internet Research*.

Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth violence and juvenile justice*, *4*(2), 148-169.

Pearce, J. J. (2014). 'What's Going On'to Safeguard Children and Young People from Child Sexual Exploitation: A Review of Local Safeguarding Children Boards' Work to Protect Children from Sexual Exploitation. *Child abuse review*, *23*(3), 159-170.

Pew Internet & American Life Project. (2007), "Teens, Privacy & Online Social Networks. How teens manage their online identities and personal information in the age of MySpace".
www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Privacy_SNS_Report_Final.pdf (Apr. 21, 2019)

Pew Internet & American Life Project. (2009). "Teens and Sexting. How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging". http://pewInternet.org/Reports/2009/Teens-and-Sexting.aspx(Apr. 21, 2019).

Porter, L., & Coggin, W. (1995). Research strategies in technical communication (No. 001.4 P846). John Wiley & Sons.

Power, A., & Morison, J. (2014). The rise of the digital citizen-stakeholder: rebalancing multistakeholder governance.

PSHE Association. (2016). Key Principles of Effective Prevention Education London: PSHE Association.

Pūraitė, A., &Prokofjeva, N. (2019). Policy of European Union on the Safety of Children in Cyber Space.

Q, Li. (2006). Cyberbullying in schools: A research of gender differences. *School psychology international*, *27*(2), 157-170.

Rains, S. A., & Brunner, S. R. (2015). What can we learn about social network sites by studying Facebook? A call and recommendations for research on social network sites. *New media & society*, *17*(1), 114-131.

Rana, N. P., Williams, M. D., & Dwivedi, Y. K. (2013, March). Examining Factors Affecting Adoption Of Online Public Grievance Redressal System: A Case Of India. In *UKAIS* (p. 31).

Research in Practice and University of Greenwich (2015). Working effectively to address Child Sexual Exploitation: A briefing Totnes: Research in Practice

Ribble, M., & Bailey, G. D. (2011). Digital citizenship in schools. International Society for Technology in Education.

Richards, R., McGee, R., Williams, S. M., Welch, D., &Hancox, R. J. (2010). Adolescent screen time and attachment to parents and peers. *Archives of pediatrics & adolescent medicine*, *164*(3), 258-262.

Rizo, C. F., Klein, L. B., Chesworth, B. R., O'Brien, J. E., Macy, R. J., Martin, S. L., ... & Love, B. L. (2019). Educating youth about commercial sexual exploitation of children: A systematic review. *Global Social Welfare*, *6*(1), 29-39.

Robertson, J. (2000). The three Rs of action research methodology: Reciprocity, reflexivity and reflection-on-reality. Educational action research, 8(2), 307-326.

Romero Moreno, F., Harbinja, E., Leiser, M., Barker, K., Mangan, D., &Dushi, D. (2019). Online Harms White Paper: Consultation Response: BILETA Response to the UK Government Consultation'Online Harms White Paper'.

Safernet. (2016). Sfaernet Brazil. https://new.safernet.org.br/ (Dec. 10, 2018).

Safenetwork.org.uk, (2014). Be aware of the potential online risks to children and youngpeople.http://www.safenetwork.org.uk/help_and_advice/Pages/potential_online_risks.aspx (Feb.20, 2019).

Sanchez, H., & Kumar, S. (2011). Twitter bullying detection. *ser. NSDI*, *12*(2011), 15.

Sawmy, K. (2013). The impact of Internet use for children and adolescents. Presentation.http://www.gov.mu/portal/sites/sid2011/files/Miss%20Sawmy.pdf (Feb. 20, 2019).

Schleicher, A. (2019). *Helping Our Youngest to Learn and Grow: Policies for Early Learning. International Summit on the Teaching Profession*. OECD Publishing. 2, rue Andre Pascal, F-75775 Paris Cedex 16, France.

Seto, M. C. (2017). Research on online sexual offending: what have we learned and where are we going?. *Journal of sexual aggression*, *23*(1), 104-106.

Shahidullah, Shahid, M. (2017). Criminalization of child abuse and violence against children in South Asia: law and legal advances in India, Pakistan, and Bangladesh. In *Crime, Criminal Justice, and the Evolving Science of Criminology in South Asia* (pp. 109-144). Palgrave Macmillan, London.

Sharp, N. (2013). Missing from discourse: South Asian young women and sexual exploitation. In *Critical Perspectives on Child Sexual Exploitation and Related Trafficking* (pp. 96-109). Palgrave Macmillan, London.

Shaw, T., Dooley, J. J., Cross, D., Zubrick, S. R., & Waters, S. (2013). The Forms of Bullying Scale (FBS): Validity and reliability estimates for a measure of bullying victimization and perpetration in adolescence. *Psychological assessment*, *25*(4), 1045.

Shipton, L. (2011). Improving e-safety in primary schools: a guidance document. *hallamunion. ac. uk/_assets/pdf/improving-esafety-in-primary. Pdf*(Apr., 16, 2021).

Shin, W. (2015). Parental socialization of children's Internet use: A qualitative approach. *New media & society*, *17*(5), 649-665.

Shin, W., & Lwin, M. O. (2017). How does "talking about the Internet with others" affect teenagers' experience of online risks? The role of active mediation by parents, peers, and school teachers. *New Media & Society*, *19*(7), 1109-1126.

Sidebotham, P., Brandon, M., Bailey, S., Belderson, P., Dodsworth, J., Garstang, J., ... & Sorensen, P. (2016). *Pathways to harm, pathways to protection: a triennial analysis of serious case reviews 2011 to 2014*. Department for Education.

Singh, R. D. (2018). Mapping online child safety in Asia and the Pacific. *Asia & the Pacific Policy Studies*, *5*(3), 651-664.

Smeaton, E. (2013). Running from hate to what you think is love: The relationship between running away and child sexual exploitation. *Barnardo's*.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., &Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of child psychology and psychiatry*, *49*(4), 376-385.

Soh, P. C. H., Chew, K. W., Koay, K. Y., & Ang, P. H. (2018). Parents vs peers' influence on teenagers' Internet addiction and risky online activities. *Telematics and Informatics*, *35*(1), 225-236.

Solove, D. J. The Future of Reputation: Gossip, Rumor, and Privacy on the Internet. New Haven: Yale UP, 2007.

Soumitra, D., and Beñat, B. O. (2012). The Global Information Technology Report WEForum, www3.weforum.org/docs/Global_IT_Report_2012.pdf(Apr.19,2019).

SQUID. (2016).Squid:Optimising web Delivery.www.squid-cache.org (Feb., 20, 2020).

Stanley, J., Tomison, A. M., & Pocock, J. (2003). *Child abuse and neglect in Indigenous Australian communities*. Canberra: Australian Institute of Family Studies.

Stanley, J. (2002). Child abuse and the Internet [This article is reproduced from Issues in Child Abuse Prevention, no. 15, Summer 2001.]. *Journal of the Home Economics Institute of Australia*, *9*(1), 5-27.

Steel, C. M. (2015). Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms. *Child abuse & neglect*, *44*, 150-158.

Stern, M. J., Adams, A. E., & Elsasser, S. (2009). Digital inequality and place: The effects of technological diffusion on internet proficiency and usage across rural, suburban, and urban counties. *Sociological Inquiry*, *79*(4), 391-417.

Stevanovic, D., Vlajic, N., & An, A. (2013). Detection of malicious and non-malicious website visitors using unsupervised neural network learning. *Applied Soft Computing*, *13*(1), 698-708.

Szafranski, A., Szwedo, P., & Klein, M. (2018). Comparative Perspectives of Adult Content Filtering: Legal Challenges and Implications. *Cath. UL Rev.*, *68*, 137.

Thanuskodi, S. (2019). Usage of social media among LIS students in India. In *Literacy Skill Development for Library Science Professionals* (pp. 1-24). IGI Global.

The Internet Matters. (2016).https://www.internetmatters.org/issues/ (Apr.20, 2020).

Throuvala, M. A., Griffiths, M. D., Rennoldson, M., &Kuss, D. J. (2019). School-based prevention for adolescent internet addiction: Prevention is the key. A systematic literature review. *Current neuropharmacology*, *17*(6), 507-525.

Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K., &Sirivianos, M. (2016, October). Cyber security risks for minors: a taxonomy and a software architecture. In *2016 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP)* (pp. 93-99). IEEE.

UNICEF.(2012). Child Safety Online, Global Challenges and Strategies, www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf(Apr.20, 2019).

UNICEF. (2016). Children's Rights and the Internet from Guidelines to Practice Articles from the Guardian Sustainable Business Child Rights Hub. https://www.unicef.org/csr/files/Childrens_Rights_and_the_Internet_Guidelines_to_Practice_Guardian_Sustainble_Business_English.pdf (Apr.20, 2019).

UNICEF.(2017).Child online protection in India. https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf (Apr.20, 2019).

UINFC2. (2013). Engaging users in preventing and fighting cyber Crime, DG Home Affairs: Prevention of and Fight against Crime ISEC 2013 Programme. www.uinfc2.eu/wp/wp-content/uploads/2014/12/UINFC2_D1.1-Cybercrime_Threats_and_Patterns.pdf (Aug., 10, 2021).

US Department of Justice (2002), Drug, Youth and the Internet. www.justice.gov/ndic/pubs2/2161/2161p.pdf (Apr.20,2019).

UK Council for Child Internet Safety. (2016) Sexting in Schools and Colleges: Responding to incidents and safeguarding young people London: UK Council for Child Internet Safety.

UK Department for Children. Schools and Families, and Department for Culture, Media and Sport (2009). "The Impact of the Commercial World on Children's Wellbeing: Report of an Independent Assessment". http://publications.dcsf.gov.uk/eOrderingDownload/00669-2009DOM-EN.pdf

US FCC (Federal Communications Commission). (2009). "In the Matter of Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming", MB Docket No. 09-26. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-69A1.pdf(Apr.18, 2018).

Valentine, G. (2017). *Public space and the culture of childhood*. Routledge.

Valenzuela, S., Park, N., & Kee, K. F. (2009). Is there social capital in a social network site?: Facebook use and college students' life satisfaction, trust, and participation. *Journal of computer-mediated communication*, *14*(4), 875-901.

VGTF. (2017). Combating child online sexual abuse. https://virtualglobaltaskforce.com/wp-content/uploads/2017/11/VGT-factsheet-English.pdf. (Mar. 20, 2019).

Vinter, K., &Siibak, A. (2012). The role of significant others in guiding pre-school children's new media usage: analysing perceptions by Estonian children and parents. *Preschool and Primary Education*, 78-94.

Wachs, S., Pan, C. C., & Wolf, K. D. (2012). Cybergrooming: Risk factors, coping strategies and associations with cyberbullying. *Psicothema*.

Wachs, S., Jiskrova, G. K., Vazsonyi, A. T., Wolf, K. D., & Junger, M. (2016). A cross-national study of direct and indirect effects of cyberbullying on cybergrooming victimization via self-esteem. *Psicologiaeducativa*, *22*(1), 61-70.

Ward, J., & Patel, N. (2006). Broadening the discussion onsexual exploitation': ethnicity, sexual exploitation and young people. *Child Abuse Review*, *15*(5), 341.

Webster, S., Davidson, J., &Bifulco, A. (2014). *Online offending behaviour and child victimisation: New findings and policy*. Palgrave Macmillan.

Wei, S., Guo, J., Yu, Z., Chen, P., & Xian, Y. (2013, May). The instructional design of Chinese text classification based on SVM. In *2013 25th Chinese Control and Decision Conference (CCDC)* (pp. 5114-5117). IEEE.

West, R., White, R. W., & Horvitz, E. (2013, May). From cookies to cooks: Insights on dietary patterns via analysis of web usage logs. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 1399-1410).

Westlake, B. G., Bouchard, M., & Frank, R. (2011). Finding the key players in online child exploitation networks. *Policy & Internet*, *3*(2), 1-32.

Weston, S., & Mythen, G. (2020). Working with and negotiating 'risk': Examining the effects of awareness raising interventions designed to prevent child sexual exploitation. *The British Journal of Criminology*, *60*(2), 323-342.

Whittaker, E., & Kowalski, R. M. (2015). Cyberbullying via social media. *Journal of school violence*, *14*(1), 11-29.

Whittle, H. C., Hamilton-Giachritsis, C., & Beech, A. R. (2013). Victims' voices: The impact of online grooming and sexual abuse. *Universal Journal of Psychology*, *1*(2), 59-71.

Whittle, H. C., Hamilton-Giachritsis, C. E., & Beech, A. R. (2014). "Under his spell": Victims' perspectives of being groomed online. *Social Sciences*, *3*(3), 404-426.

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. *Aggression and violent behavior*, *18*(1), 62-70.

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of young people's vulnerabilities to online grooming. *Aggression and violent behavior*, *18*(1), 135-146.

Willett, P. (2006). The Porter stemming algorithm: then and now. *Program*.

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2010). Online "predators" and their victims: Myths, realities, and implications for prevention and treatment.

Wolak, J., Mitchell, K. J., &Finkelhor, D. (2006). Online Victimization of Youth: Five Years Later.www.unh.edu/ccrc/pdf/CV138.pdf (Apr.13, 2018).

Wortley, R., &Smallbone, S. (2012). *Internet child pornography: Causes, investigation, and prevention*. ABC-CLIO.

Xu, Q., & Liu, Z. (2008, October). Automatic Chinese text classification based on NSVMDT-KNN. In *2008 Fifth International Conference on Fuzzy Systems and Knowledge Discovery* (Vol. 2, pp. 410-414). IEEE.

YISS. (2011). Youth Internet Safety study. unh.edu/ccrc/pdf/YISS_Methods_Report_final.pdf (Mar.20 2019).

YPRT (Youth Protection Roundtable). (2009), Stiftung DigitaleChancen. Youth Protection Toolkit. www.yprt.eu/transfer/assets/final_YPRT_Toolkit.pdf (Jan. 10, 2019).

Zabatiero, J., Straker, L., Maacmantilla, A., Edwards, S., & Danby, S. (2018). Young children and digital technology: Australian early childhood education and care sector adults' perspectives. *Australasian Journal of Early Childhood*, *43*(2), 14-22.

Zainudin, A. (2012). Research methodology and data analysis. *Malaysia: Published by deesega*.

Zhang-Kennedy, L., Chiasson, S., & van Oorschot, P. (2016, June). Revisiting password rules: facilitating human management of passwords. In *2016 APWG symposium on electronic crime research (eCrime)* (pp. 1-10). IEEE.

Zhang, X., Tong, J., Vishwamitra, N., Whittaker, E., Mazer, J. P., Kowalski, R., ... & Dillon, E. (2016, December). Cyberbullying detection with a pronunciation based

convolutional neural network. In *2016 15th IEEE international conference on machine learning and applications (ICMLA)* (pp. 740-745). IEEE.

Zhao, R., & Mao, K. (2016). Cyberbullying detection based on semantic-enhanced marginalized denoising auto-encoder. *IEEE Transactions on Affective Computing*, *8*(3), 328-339.

Zhuang, H., Wang, C., Li, C., Wang, Q., & Zhou, X. (2017, June). Natural language processing service based on stroke-level convolutional networks for Chinese text classification. In *2017 IEEE international conference on web services (ICWS)* (pp. 404-411). IEEE.

Zych, I., Ortega-Ruiz, R., & Del Rey, R. (2015). Systematic review of theoretical studies on bullying and cyberbullying: Facts, knowledge, prevention, and intervention. *Aggression and violent behavior*, *23*, 1-21.

APPENDICES

Appendix I: Consent Form for Participation in Research

National Institute of Technology Karnataka, Surathkal

Consent Form for Participation in Interview Research

I volunteer to participate in a research study conducted by Dittin Andrews from NITK Surathkal. I understand that this study is designed to gather information related to Children Online Safety Issues

1. I have been given sufficient information about this research project. The purpose of my participation in this study has been explained to me and is clear.
2. My participation in this study is voluntary, and I am free to withdraw at any time without giving any reason. In addition, if I am uncomfortable to answer any particular question or questions, I am free to decline or end the survey. If I decline to participate or withdraw from the study, it will not be disclosed.
3. I understand extracts from the studywill be kept as confidential and used only for the academic purpose.
4. I have read and understood the explanation provided to me, I have had all my questions answered to my satisfaction, and I voluntarily agree to participate in this study.

_____ _____

Participant's Signature Signature of the witness

_____

Signature of the Investigator

Appendix II: Questionnaire For Students

A. Demographic Questions.

1. Location ……..

Please put a (√) mark to indicate your Preference and the precise response for respective questions.

2. Gender Male ☐ Female ☐

3. Age

A. 8-10 years B. 10 – 12 years C. 12 – 15 years D. Above 15 years

4. Occupation

A. Student B. Joined C. School Drop–out D. Uneducated

5. Parent's Occupation

A. Employed B. Self–employed C. Student D. Unemployed

E. Agriculture F. Others (…..)

6. Annual Income of the Family Below

A. Rs. 1,00,000/- B. Rs.1,50,000/- to Rs.2,00,000/- Rs.1,00,000

Rs. 2,00,000/- to Rs 2, 50, 000 C. Rs. 2, 50, 000/- to Rs. 3,00,000/-

DRs.3, 00,001 – and above

7 Present place of residence

A. Village B. Town C. City

8. Size of the family

A. 1-2 Member B. 2-4 Member C. Member D. Above 6 Member

9. Type of current residence

A. Own house B. Rental

10. Parents awareness about internet technologies

A. Yes B. No

11. Parents awareness about Social Networking Sites

A. Yes B. No

12. Parents awareness about E-learning tools

A. Yes B. No

13. Do you use the Internet for online (data or information) access

A. Yes B. No

14. How often you use the Internet (weekly)

A. Every day B. Sometimes C. Not at all D. Cannot say

15. Which device do you use for online content access or internet use?

A. CPU./ Computer B. Mobile

16. Duration of internet usages (daily)

G. Less than an hour H. 1-2 hours I. More than 2 hours

17. Frequency of use pattern

A. Education-related content search B. Socialization C. Entertainment (Videos)

D. Games E. Others (Specify…..)

18. Do you use Social Networking Sites?

A. Yes B. No

19. In which Social Networking Site do you engage more?

A. Facebook B. Twitter C. LinkedIn D. Instagram

E. WhatsApp F. Google Hangout G. MySpace H. Other …….

20. How often do you use a Social Networking Site?

A. Daily B. Rarely C. All the time

D. Once a week E. Twice a week F. Never

21. What is the average time spent every time you log in to any Social Networking Site?

A. less than 5 Minutes B. 5 – 15 Minutes C. 15 – 30 Minutes

D. 30 – 60 Minutes E. More than 1 Hour

22. Do you get influenced by online promotional ads related to different purposes?

A. Yes B. No

23. What is the age group of the people you connect with over internet platforms or certain socializing platforms?

A. Less than 10 years B. 10 – 15 years C. 15 – 20 years

D. 20 – 25 years E. 25- 35 years F. More than 35 years

24. What type of conversation that you make with your online friends?

A. Text – Chat B. Audio conversation C. Video calling

25. Do you read the review about the online website and its purposes before signing up with them?

A. Yes B. No

26. What type of personal information do you upload when pre- signup or post- sign-in?

1. Name	A. Yes	B. No
2. E-mail	A. Yes	B. No
3. Location	A. Yes	B. No
4. Education	A. Yes	B. No
5. Family Background	A. Yes	B. No
6. Relation/ Relatives	A. Yes	B. No
7. Social Preferences	A. Yes	B. No
8. Interests	A. Yes	B. No
9. Payment Details or sources	A. Yes	B. No

27. How continuously do you use an Application or Web platform when being online?

A. Less than 5 Minutes b. 5 – 15 Minutes C. 15 – 30 Minutes

D. 30 – 60 Minutes E. More than 1 Hour.

28. Did you ever experience system hang- up / or auto camera ON mode when accessing online content?

A. Yes B. No

29. Did you ever experience a forcible recommendation for update or installation by a third-party app or website?

A. Yes B. No

30. Does your browser ask you (whether) to save or use your cookies and search details?

A. Yes B. No

31. Did you have experience with any mischievous act by any person online?

A. Yes B. No

What was the nature of the act? Please Specify (…….)

32. Did you ever felt uncomfortable, upset, or feel that you should not have seen it?

A. Yes B. No

What was the nature of the act? Please Specify (……)

Online Preference to the Social Networking Sites for personal purpose

		Strongly disagree	Disagree	Neutral	Strongly Agree
33.	Facebook	☐	☐	☐	☐
34.	LinkedIn	☐	☐	☐	☐
35.	WhatsApp	☐	☐	☐	☐

36.	Instagram	☐	☐	☐	☐
37.	Twitter	☐	☐	☐	☐
38.	Google Plus	☐	☐	☐	☐
39.	My Space	☐	☐	☐	☐
40.	Gaming platforms	☐	☐	☐	☐
41.	Others (……)	☐	☐	☐	☐

B. Descriptive Questions

Please put a (√) mark to indicate your Preference and the precise response for respective questions.

a) The Purpose of using the Internet or online platforms

		Strongly disagree	Disagree	Neutral	Strongly Agree
42.	Share the information with many people at once	☐	☐	☐	☐
43.	Seeing photos/ videos	☐	☐	☐	☐
44..	Receiving updates or comments	☐	☐	☐	☐
45.	Viewing funny / entertaining Videos/posts	☐	☐	☐	☐
46.	Update with news & events	☐	☐	☐	☐
47.	To Help/ support others	☐	☐	☐	☐

48.	To Get help/ support from others	☐	☐	☐	☐
49.	Receive feedback from others	☐	☐	☐	☐
50.	To get news and updates about different products and services	☐	☐	☐	☐
51.	To get daily social–economic development news to make better buying decision	☐	☐	☐	☐
52.	Educational information or project-related information	☐	☐	☐	☐
53.	It is significant supporting future academic accomplishments	☐	☐	☐	☐

b)	Types of content	Strongly disagree	Disagree	Neutral	Strongly Agree
54.	Blog / Bulletins ☐		☐ ☐	☐	
55.	Community Discussion	☐	☐	☐	☐
56.	Profile	☐	☐	☐	☐
57.	Messages/Chat/Video calling	☐	☐	☐	☐

58.	Educational resource access	☐	☐	☐	☐
59.	Music	☐	☐	☐	☐
60.	Events	☐	☐	☐	☐
61.	Tweet / Comment	☐	☐	☐	☐
62.	Grab/ Copy/ Share	☐	☐	☐	☐
63.	Forums/ Groups	☐	☐	☐	☐
64.	Videos	☐	☐	☐	☐
65	Others	☐	☐	☐	☐

c) Need of Online/ Internet Platform

		Strongly disagree	Disagree	Neutral	Strongly Agree
66.	It enables socializing irrespective of location and other demographic constructs across the world	☐	☐	☐	☐
67.	It helps in getting information about subject matters (Educational)	☐	☐	☐	☐

68.	It helps in making better carrier decision and reviews	☐	☐	☐	☐
69.	It helps in knowing the world and activities better.	☐	☐	☐	☐
70.	Internet facility helps students in getting more suitable and significant e- learning contents	☐	☐	☐	☐
71.	It helps in getting education & personality development approaches	☐	☐	☐	☐
72.	Social media helps the students to do their assignments, projects and other relevant information	☐	☐	☐	☐

d) Need for cybercrime avoidance measures

	Strongly disagree	Disagree	Neutral	Strongly Agree

73.	Cybercrime avoidance solutions can help in preserving personal details	☐	☐	☐	☐
74.	It can help children to be away from suspicious activities or contents affecting moral as well as social nature	☐	☐	☐	☐

e) Possible Cybercrime avoidance measures

		Strongly disagree	Disagree	Neutral	Strongly Agree
75.	Limited access time to the Children	☐	☐	☐	☐
76	Advanced content filtering	☐	☐	☐	☐
77	Demographic variable based (age/gender) content filleting	☐	☐	☐	☐
78	Log-based parental control and auto- information exchange	☐	☐	☐	☐

79	Cyber counseling	☐	☐	☐	☐
80.	User – centric log- analysis and information exchange (based on frequent search pattern)	☐	☐	☐	☐
81.	Access denial to the in-system memory space or data (i.e. application access denial to the internal/ external memory and other details such as cookies,contact details, image or video saved)	☐	☐	☐	☐
82.	Pre – audit of the mobile applications as well as websites for transparent service provision	☐	☐	☐	☐

Appendix III: Questionnaire For Parents

A. Demographic Questions.

1. Location ……..

Please put a (√) mark to indicate your Preference and the precise response for respective questions.

2. Gender Male ☐ Female ☐

3. Age

A. 20-30 years B. 30 – 40 years C. 40 – 50 years D. Above 50 years

4. Occupation

A. Employed B. Self–employed C. Student D. Unemployed

E. Agriculture F. Others (…..)

5. Annual Income

Below. B. Rs.1,00,000/- C. Rs. 1,50,000/- to Rs. 2,00,000/-
Rs. 1,00,000/- to Rs. 1,50,000/-

Rs. 2,00,000/- tD. Rs. 2,50,000/- E. Rs. 3,00,000/- and above
Rs. 2,50,000/- to Rs. 3,00,000/-

6. Place of residence

A. Village B. Town C. City

7. Size of the family

A. 1-3 Member B. 2-5 Member C. Member D. Above 6 Member

8. Type of current residence

A. Own house B. Rental

9. Awareness about internet technologies

A. Yes B. No

10. Awareness about Social Networking Sites

A. Yes B. No

11. Awareness about E-learning tools and technologies (children dependency on e-learning)

A. Yes B. No

12. How often do you use the Internet (weakly)

A. Every day B. Sometimes C. Not at all D. Cannot say

13. Which device do you use for online content access or internet use?

A. CPU./ Computer B. Mobile

14. How often have you given (or your kid asks) your phone to the child?

A. Sometimes B. Whenever he/she asks for it

15. Duration of internet usages (daily)

A. Less than an hour B. 1-2 hours C. More than 2 hours

16. Frequency of use pattern

A. Education related content search B. Socialization C. Entertainment (Videos)

D. Games E. Others (Specify…..)

17. Do you monitor for what purpose your kid uses internet facilities and mobile?

A. Yes B. No

18. Do you check log details after your kid uses a phone or computer?

A. Yes B. No

19. Do you ask your kid whom and which type of content does he/she access and for what purpose?

A. Yes B. No

20. Do you use any Social Networking Site?

A. Yes B. No

21. In which Social Networking Site do you engage more?

A. Facebook B. Twitter C. LinkedIn D. Instagram

E. WhatsApp F. Google Hangout G. MySpace H. Other …….

22. How often do you use Social Networking Sites?

A. Daily B. Rarely C. All the time

D. Once a week E. Twice a week F. Never

23. What is the average time your child spent on any Social Networking Site or internet services?

A. less than 15 Minutes B. 15 -30Minutes C. 30- 60 Minutes

D. More than 1 Hour E. I do not care

24. Have you ever got any feedback or query of online misbehave or crime by your children?

A. Yes B. No

25. Do you monitor the log details of your kid and their socio-behavioral changes throughout internet access (or after using internet access)?

A. Yes B. No

26. What type of conversation does your child make when using internet access and a phone?

A. Text – Chat B. Audio conversation C. Video calling

27. Did your kid even complain about online fraud/cheating/blackmailing/threat etc.?

A. Yes B. No

28. Do you believe that frequent search pattern filtering and parental control can effectively avoid provable cybercrime?

A. Yes B. No

29. Would you prefer getting (Internet) access details of your kids?

A. Yes B. No

30. Are you aware of cybercrime?

A. Yes B. No

31. Prevailing predefined or dedicated e-learning media such as mobile and computer with predefined content filtering provision and log detail auto-update can help avoid kids to incline in a negative direction?

A. Yes B. No

C. Descriptive Questions

Please put a (√) mark to indicate your Preference and the precise response for respective questions

		Strongly disagree	Disagree	Neutral	Agree	Strongly Agree
32.	The ability for using computers and the Internet effectively entails good interpersonal associations and encourages imagination, self-expression, and independently identify creation	☐	☐	☐	☐	☐
33.	It is also significant in reinforcing a sense of belonging or social networking and contributes to the growth of digital social skills	☐	☐	☐	☐	☐
34.	Avoiding unwanted contact can reduce the risk of cyber solicitation and allied crime	☐	☐	☐	☐	☐
35.	Reducing unwanted online habits can avoid cybercrime significantly	☐	☐	☐	☐	☐
36.	It was confining children to the home- and furnishing them with media and technology that will make the child's bedroom	☐	☐	☐	☐	☐

	a more attractive alternative to the outside world's apparent dangers.					
37.	Confining children to the home and furnishing them with media and technology can invite the possibility of stranger danger	☐	☐	☐	☐	☐
38.	Reducing online risk may curb online opportunities	☐	☐	☐	☐	☐
39.	Pornography contents online incite violence of various kinds	☐	☐	☐	☐	☐
40.	Pornography and other similar material would include 'hate sites' and material that appears to encourage or celebrate forms of self-harm.	☐	☐	☐	☐	☐
41.	The majority of parents encourage their children's early access to the Internet by yielding their chances to explore and play online	☐	☐	☐	☐	☐
42.	The sex sites were retrieved by accident when a child, often in the process of doing homework, used a harmless word to search for information or pictures	☐	☐	☐	☐	☐
43.	Pornography and sexualized material can influence the moral values, sexual attitudes	☐	☐	☐	☐	☐

	of children and youth, including their attitudes toward sexual violence.					
44.	The Internet has a positive impact on their children's advancement in school, as well as on preparation for professional life	☐	☐	☐	☐	☐
45.	Children and young people keep in touch with each other via instant messengers, webcams, and social network sites; unfortunately for some children, it brings negative shades because of hurtful messages and bullying.	☐	☐	☐	☐	☐
46.	Restrict access to certain web pages can avoid cyberbullying and crimes.	☐	☐	☐	☐	☐
47.	Teaching them responsible behavior on the web, making them aware of the dangers they might face, and prevent the incidence of online risks can help in reducing cybercrime.	☐	☐	☐	☐	☐
48.	Avoiding the perception that enabling children with Internet-connected devices is a sign of socio-economic status can help to reduce cyberbullying	☐	☐	☐	☐	☐

49.	Avoiding grooming and offender by denying the parent's trust can help to avoid cyber abuse.	☐	☐	☐	☐	☐
50.	Identifying which circumstances pose what kind of risk, which factors mean that risk is increased or reduced, and when risks do not result in tangible harm can avoid cyber child abuse.	☐	☐	☐	☐	☐
51.	Parents must begin educating their children at home about the risks associated online and take defensive methods on the safety of their devices at home.	☐	☐	☐	☐	☐
52.	Avoid children downloading applications without their permission.	☐	☐	☐	☐	☐
53.	Enabling web personalization data and sharing it with local administrative agencies or monitoring agencies can help avoid online and offline predators.	☐	☐	☐	☐	☐
54.	Parental control softwares for restricting app installation or use can also be a vital solution	☐	☐	☐	☐	☐

Appendix IV: Questionnaire For Technical Experts

A. Demographic Questions.

1. Location ……..

Please put a (√) mark to indicate your Preference and the precise response for respective questions.

2. Gender Male ☐ Female ☐

3. Age

A. 20-30 years B. 30– 40 years C. 40 – 50 years D. Above 50 years

4. Occupation

A. Student B. Joined C. School Drop–out D. Uneducated

5. Parent's Occupation

A. Employed B. Self–employed C. Student D. Unemployed

E. Agriculture F. Others (…..)

6. Annual Income of the Family Below

Below A. Rs. 1,50,0000/-to B. Rs. 2,50,000/- to Rs. 4,00,000/-

` Rs. 1,50,000/- Rs. 2,50,000/-

Rs. 4,00,000/- C. Rs. 5,50,000/- to D. Rs. 6,00,001/- and above

Rs.5,50,000/- Rs. 6,00,000/-

7 Place of residence

A. Village B. Town C. City

8. Awareness about internet security (filtering and content blocking) technologies

A. Yes B. No

9. Awareness about social Networking Sites and allied content security

A. Yes B. No

10. Awareness about parental control for cybercrime

A. Yes B. No

11. Do you have experience in internet content-use monitoring over mobile or computer systems?

A. Yes B. No

12. Do you think content filtering/abstraction and parental control can help to avoid cyberbullying?

A. Yes B. No

13. Which Social Networking Site do you think can have more cyberbullying probability?

A. Facebook B. Twitter C. Linkedln

D. Instagram E.WhatsApp F. Google Hangout

G. MySpace H. Other ……..

14. Does your organization considers cybercrime and allied factors to be dealt with strictly by enabling children-sensitive content filtering and blocking provision?

A. Yes B. No

15. Do you monitor the log details of your kid and their socio-behavioral changes throughout internet access (or after using internet access)?

A. Yes B. No

16. Which type of content as communication media can have more proneness for cybercrime or bullying?

A. Text-Chat B. Audio conversation C. Video calling

17. Can content-sensitive session control and content-filtering be an effective measure of avoiding cyber children crime (online fraud/cheating/blackmailing/threat, etc.)?

A. Yes B. No

18. Do you believe that frequent search pattern filtering and parental control can effectively avoid any potential cybercrime?

A. Yes B. No

19. Can be enabling predefined or dedicated 3-learning media such as mobile and computer with predefined content filtering provision and log detail auto-update can help avoid kids incline in the negative direction.

A. Yes B. No

20. Can the content monitoring and filtering (URL, content search, keyword, demographic sensitive filtering) approach effectively avoid pornography and allied online children exploitation Cases?

A. Yes B. No

19. Descriptive Questions

Please put a (√) mark to indicate your preference and the precise response for respective questions

a) Cyber Crime avoidance

20.	Avoiding unwanted contact can reduce the risk of cyber solicitation and allied crime	☐	☐	☐	☐	☐
21	Reducing unwanted online habits can avoid cybercrime significantly	☐	☐	☐	☐	☐
22	It was confining children to the home and furnishing them with media and technology that will make the child's bedroom a more attractive alternative to the apparent dangers of the outside world.	☐	☐	☐	☐	☐
23	Strict content monitoring and filtering (URL, content search, keyword, demographic sensitive filtering) effectively avoid pornography and allied online children exploitation cases.	☐	☐	☐	☐	☐
24.	Providing predefined or dedicated 3-learning media such as mobile and computer with predefined content filtering provision and log detail auto-update can help avoid kids to incline in a negative direction.	☐	☐	☐	☐	☐

25	Frequent search pattern filtering and parental control can be effective solutions.	☐	☐	☐	☐	☐
26	Content–sensitive session control and control-filtering can be an effective measure to avoid cyber children crime (online fraud/cheating/blackmailing/threat etc.)	☐	☐	☐	☐	☐
27.	Monitor the log details of your kid and their socio-behavioral changes throughout internet excess.	☐	☐	☐	☐	☐
28.	Enabling content block provision with the internet service provider can help to curb child online exploitation or harassment issues.	☐	☐	☐	☐	☐
29.	Providing link-block option with browser to avoid accidentally seen pornographic contents forwarded by else can curb child online harassment for bullying	☐	☐	☐	☐	☐
30.	Providing auto information exchange for web access can help to prohibit children from coming in contact with bullying elements, or groomers can avoid cyber children exploitation or blackmail	☐	☐	☐	☐	☐
31.	Avoiding grooming and offender by denying the parent's trust can help to avoid cyber abuse.	☐	☐	☐	☐	☐

32.	Exploiting demography information such as location, age, precious search patterns, and allied uses personalization variables can help update parents and children to avoid unwanted (harmful) contacts.	☐	☐	☐	☐	☐
33.	Identifying which circumstances pose what kind of risk, which factors mean that risk is increased or reduced, and when risks for or do do not result in tangible harm can avoid cyber child abuse can help to curb the online child exploitation problem	☐	☐	☐	☐	☐
34.	Avoiding third-party applications from auto-download and media (phone data) access without permission can help to avoid private data loss and further defamation	☐	☐	☐	☐	☐
35.	I am avoiding any spreading of malicious viruses to disrupt the activities of other internet users.	☐	☐	☐	☐	☐
36.	Developing Groomer's identification system using advanced web personalization can help to curb online child exploitation or further offline offense(probability)	☐	☐	☐	☐	☐
37.	Online Identification of online grooming, which is a private interaction between the grooms and their victims, can help to avoid cybercrime	☐	☐	☐	☐	☐

38.	Applying web personalization, potential threats towards online child abuse can be identified.	☐	☐	☐	☐	☐
39	Enabling anti-recording or replication features when online communication (vide calling or multimedia sharing) can help avoid online child abuse, blackmailing, and exploitation.	☐	☐	☐	☐	☐
40.	Exploiting spatial and temporal relationships between offenders can help identify possible offenders.	☐	☐	☐	☐	☐
41.	Identifying the commercial market and its circuit can help prohibit children's online sexual exploitation or allied events.	☐	☐	☐	☐	☐
42.	Handling both commercial child exploitation as well as non-commercial exploitation can help to avoid an upsurge in cybercrime	☐	☐	☐	☐	☐
43	Filtering online pornography; violent video games: websites that espouse racial or ethnic hatred: commercial sites can play a vital role in avoiding online child abuse or exploitation	☐	☐	☐	☐	☐
44.	ICT can help human traffickers may also recruit new victims, including children and market child sex tourism and hence identifying such activities using web-mining and	☐	☐	☐	☐	☐

	personalization can help to eradicate such issue					
45.	Cyber-bullies may use public websites and social media to broaden their audience and increase the impact on victims and hence detecting such events can be vital.	☐	☐	☐	☐	☐
46.	Filters or 'parental controls can be installed on an individual computer or configured at the ISP level	☐	☐	☐	☐	☐
47.	At a higher level, ISPs can block content originating from specific IP addresses found to distribute content, such as child abuse images.	☐	☐	☐	☐	☐
48.	Including the ability of or justification for ISPs to determine whether the content was illegal and block lists' transparency can help avoid online children exploitation.	☐	☐	☐	☐	☐
49.	Using advanced techniques, including keyword and phrase searches to help screen out offensive content that has not been included on a black or exclusive list, can help to filter offensive content (to curb the issue of online child exploitation).	☐	☐	☐	☐	☐
50.	Providing parents software to monitor activities such as computer programs, websites visited, chat room activity, and social network	☐	☐	☐	☐	☐

	sites accessed can help avoid kids indulging in inappropriate links.					
51.	Built-in mechanisms to prevent children from bypassing or circumventing the filter, including password protection and other devices to prevent children from uninstalling the product or changing the settings.	☐	☐	☐	☐	☐
52.	Enabling web personalization data and sharing it with local administrative agencies to monitoring agencies can help avoid online and offline predators.	☐	☐	☐	☐	☐
53.	Parental control softwares to restrict app installation or use can also be a robust solution.	☐	☐	☐	☐	☐
54.	Parental control features can block, restrict, limit, or allow access to different features for younger children.	☐	☐	☐	☐	☐
55.	Putting legal constraints on the current state of art recommender system can help to avoid further child online risk probability	☐	☐	☐	☐	☐

Appendix V: Questionnaire For Legal Experts

A. Demographic Questions.

1. Location ……..

Please put a (√) mark to indicate your Preference and the precise response for respective questions.

2. Gender Male ☐ Female ☐

3. Age

A. 20-30 years B. 30– 40 years C. 40 – 50 years D. Above 50 years

4. Occupation

A. Employed B. Self–employed C. Student D. Unemployed

E. Agriculture F. Others (…..)

5. Annual Income of the Family Below

Below A. Rs. 1,50,0000/-to B. Rs. 2,50,000/- to Rs. 4,00,000/-

` Rs. 1,50,000/- Rs. 2,50,000/-

Rs. 4,00,000/- C. Rs. 5,50,000/- to D. Rs. 6,00,001/- and above

Rs.5,50,000/- Rs. 6,00,000/-

6. Place of residence

A. Village B. Town C. City

7. Awareness about internet security (filtering and content blocking) technologies

A. Yes B. No

8. Awareness about social Networking Sites and allied content security

A. Yes B. No

9. Do you have awareness about cybercrime avoidance policies and rules and regulations in India?

A. Yes B. No

10. Do you think current policies for online child crime or bullying avoidance are sufficient?

A. Yes B. No

11. Do you think there must be a multiparty synchronized process and allied regulation to identify predators and groomers to avoid online child exploitation?

A. Yes B. No

D. Descriptive Questions

Please put a (√) mark to indicate your Preference and the precise response for respective questions

a) Cyber Crime avoidance

12.	Making strict regulations for content monitoring and filtering (URL, content search, keyword, demographic sensitive filtering) approach effectively avoids pornography and allied online children exploitation cases.	☐	☐	☐	☐	☐

13.	Providing strict and non-negotiable regulations for both ISP and phone manufacturers to ensure data exchange and unauthorized access can help curb online child exploitation, bullying, or blackmailing cases.	☐	☐	☐	☐	☐
14.	Making rules for auto information exchange for web access can help prohibit children from contacting bullying elements or groomers to avoid cyber children exploitation or blackmailing.	☐	☐	☐	☐	☐
15.	Involving private-public partnerships and exploiting the most advanced technologies can help identify predators and make rules to observe the predators' activities to avoid many abuse cases.	☐	☐	☐	☐	☐
16.	Making strict and special cells for identifying the commercial market and its circuit can help prohibit children's online sexual exploitation or allied events.	☐	☐	☐	☐	☐
17.	Handling both commercial child exploitation and non-commercial exploitation can help avoid a surge in online child exploitation.	☐	☐	☐	☐	☐
18.	Enabling web personalization data and sharing it with local administrative agencies or monitoring agencies can help avoid online and offline predators.	☐	☐	☐	☐	☐

19	Education, health systems, law enforcement, and child protection workers should include internet solicitation in their areas of expertise so that they may provide the support and advice needed to counsel individuals who have experienced online solicitation	☐	☐	☐	☐	☐
20.	Content risk, the Internet is largely unregulated because governments cannot enforce laws and use the police. Hence applying multiparty synchronized activities can help swift predator identification and action to avoid any hazardous consequences.	☐	☐	☐	☐	☐
21.	Only cyber-crime is universally acknowledged in its various forms, such as spreading malicious viruses to disrupt the activities of other internet users. However still, moral guidelines are needed to deal with the problem.	☐	☐	☐	☐	☐
22.	There is the need to ban websites or similar platforms that promote such content.	☐	☐	☐	☐	☐
23.	Governments should pay extra attention to is the development of policies and practices aimed at ensuring safety and protection for participants of the network, especially the youngest ones.	☐	☐	☐	☐	☐
24.	Putting legal constraints on the current state of art recommender system can	☐	☐	☐	☐	☐

	help avoid further child online risk probability.					
25.	Taking strict action against child exploitation, child pornography, and content sharing can avoid major issues.	☐	☐	☐	☐	☐
26.	In most countries, laws against child sexual abuse material are based on the policy position. Children should be protected from commercial sexual activities because they are too young to give informed and thus valid consent.	☐	☐	☐	☐	☐
27.	Interests protected by the criminalization of child abuse images include the protection of minors from abuse and the disruption of commercial markets in child abuse images, which may encourage offenders to seek to produce and supply further images	☐	☐	☐	☐	☐
28.	Practitioners need to use professional curiosity and judgment to explore what is going on with each young person.	☐	☐	☐	☐	☐
29.	Handling both commercial child exploitation as well as non-commercial exploitation can help to avoid an upsurge in cybercrime.	☐	☐	☐	☐	☐
30.	Making very strict punishment to the traffickers can help reducing child abuse and allied material production.	☐	☐	☐	☐	☐

31.	Emphasizing the functional relations between parts and whole for promoting online child safety and developing strategies in measures related to Law, Technology and procedure, Organizational structures, Capacity Building and International Cooperation.	☐	☐	☐	☐	☐
32.	Making strict rules and investigating agencies for monitoring ICT can help identify human traffickers and their activities, including children, and market child sex tourism. Identifying such activities using web-mining and personalization can help eradicate such issues.	☐	☐	☐	☐	☐
33.	A child's right to be protected from violence, abuse, and exploitation is not a choice but rather an obligation under international law.	☐	☐	☐	☐	☐
34.	Introducing strict regulations for the application developers (mobile or web) towards inappropriate access to the user's memory or activities.	☐	☐	☐	☐	☐
35.	Introducing strict punishment for cyberstalking.	☐	☐	☐	☐	☐
36.	Multi-agency approaches enable organizations to contribute their specific role while also developing shared actions to protect young people and proactively investigate abusers.	☐	☐	☐	☐	☐

37.	Safeguarding arrangements can be organized through forums such as Multi-Agency Sexual Exploitation (MASE) meetings and initiatives led by a Multi-Agency Safeguarding Hub (MASH)	☐	☐	☐	☐	☐
38.	Governments are rather slow and cannot keep the legislation and procedural basis up to date due to the rapid development of technology.	☐	☐	☐	☐	☐
39.	There should be better and strict Internet governance policies.	☐	☐	☐	☐	☐
40.	To raise the skills and capabilities of parents and children, the government should focus on delivering e-safety through the curriculum, providing teachers and the wider children's workforce with the skills and knowledge they need, reaching children and families through Extended Schools and taking steps to ensure that of sted holds the systems to account on the quality of delivery in this area	☐	☐	☐	☐	☐
41	Anonymously facilitating crime reporting prevents and investigates the reporting of crimes targeting child including pornography, identity theft, and various other crimes, including hate communication.	☐	☐	☐	☐	☐
42	Providing tips, games, and internet safety information to help the young	☐	☐	☐	☐	☐

people safety resources to teachers and professionals to safeguard to workplace and young people associated with them and finally advice for parent and caretakers for supporting children and youngsters for safe and worthy use of Internet

B I O–D A T A

DITTIN ANDREWS

Scientist E/Joint Director
Cyber Security
Centre for Development of Advanced Computing (C-DAC)
Thiruvananthapuram
Email: dittinandrews@gmail.com, dittin@cdac.in
Mob :9243033055,6360099796

- Multifaceted team player, leader, rather builder, having worked on diverse Information Security roles in managing organisation's IT Infrastructure implementation and Security, Cyber Security Research and Development, Security Audit and Compliance, IT Governance, ISMS implementation, Data Centre and Disaster Recovery site implementation and operations, HPC Security, Incident Analysis, Cyber Forensics, Managed Security Services with 19 plus years of experience.
- Played crucial role in successful delivery of flagship projects in the area of Cyber Security funded by Controller of Certifying Authorities, CERT-In, Ministry of Electronics and IT, Ministry of External Affairs, Ministry of Defense and Department of Science and Technology Government of India.
- Have played the lead role in Cyber Security Audit and Consultancy project engagements with major organizations in Banking, Non-banking, Power, Shipping and E-Governance
- An active Cyber Security professional with coveted certifications/Training in the area of Cyber Security and Invited speaker in National and International Conferences and symposiums in the area of Cyber Security.

Educational Qualifications:

- Pursuing PhD from National Institute of Technology Karnataka (Thesis submitted)
- M.C.A from Bharathidasan University, Tiruchirappalli
- Bachelor's degree in Computer Science M.G University Kottayam, Kerala

Publications:

1. An adult content identification framework: E -Discovery tools benchmark Survey, IETE International Conference on IoT, Big Data Analytics and 5G, IICI-18, 24-32, December 2018
2. International Efforts for Child Online Safety: A survey, International Journal of Web Based Communities, 16(2), 123-133, May 2020
3. Child Online Safety in Indian Context,5th IEEE International Conference on Advances in Computing & Communication Engineering, 1-4, October, 2020
4. Child Online Safety Intervention Through Empowering Parents and Technical Experts: Indian Context, International Working Conference on Transfer and Diffusion of IT (pp. 662-673). Springer, Cham,December 2020

Professional Body Membership, Fellowship and Publications:

- Fellow member -The Institution of Electronics and Telecommunications Engineers
- Young Internet Professional Fellowship under National Internet Exchange of India.
- Publications in 2 International Conferences
- Publications in 2 Scopus Indexed Journals

Industry Certifications:

- BSI Certified ISMS Lead Implementor professional
- IRCA Certified Lead Auditor for ISO 27001
- EC Council Certified Security Operations Centre Analyst
- SANS GIAC Defending Advanced Threats (Training Completed)

Major Achievements:

- Nominated as member delegate to the Benin under Multilateral Collaboration programme of Ministry of External Affairs
- Expert committee member to various organizations including IDRBT, Karnataka Cyber Forensics lab, NeSL, STQC, STPI, Kerala University, Kerala State IT Mission, BMRCL, KADCO, Canara Bank, BESCOM, CCA India
- Delivered more than 25 Invited talks and presentations in various National and International Conferences/Symposiums/Seminars conducted by reputed Academic institutions including NITs, Central Universities etc across the country
- Industry Expert for B.Voc course of Kerala University under Nation Skill Development Initiative
- Project Guidance to M.Tech/MCA/B.Tech-More than 25
- Nominated subject expert in selection committee for test engineers for STQC Bangalore
- Nominated member in review committee of Technical Assistant for STPI Bangalore

Key Skills:

- Key interest in sector specific developments in Cyber Security including banking, power, telecom
- Proactive approach and ability to take quick decisions
- Ability to work under pressure and meeting deadlines
- Good oral and written communication skills
- Development and implementation of Information Security policy, standards and guidelines
- Experience in planning and implementing technical security controls
- Understanding of Information and Cyber Security guidelines as per NCIIPC and CERT-In
- Experience in ensuring regulatory compliance as per IT Act 2000 and 2008 amendments and IT Rules 2011 (Reasonable Security Practices and Procedures) of Govt. of India
- Knowledge of various information security guidelines, standards and best practises at National Level and International Level including
    - Indian IT Act 2000 and 2008 Amendment
    - Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
    - ISO/IEC 27001:2013 Information Technology -Security techniques-ISMS Requirements
    - ISO/IEC 27001:2013 Information Technology -Security Techniques-Code of practice for Information Security Controls
    - Centre for Internet Society (CIS) controls and mapping to various standards
    - Insolvency and Bankruptcy Board of India (Information Utilities) Regulation 2017
    - Cyber Security Model Framework for Smart Cities
    - Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021
    - OWASP Top 10 Vulnerabilities
    - MITRE/SANS CWE-25
    - Reserve Bank of India Cyber Security Frameworks for Banks, NBFC, Urban Co-operative Banks
    - Cyber Security and Cyber Resilience framework for Stock exchanges, Clearing Corporation and Depositories
- Working experience in developing privacy related policies and regulations
- Knowledge in tools, technology, secure application and network design, Cyber security architecture and policy implementation

- Hands-on experience in risk assessment procedure and implementation threat and risk models as per the compliance requirement from regulatory bodies
- Hands-on experience in using and implementing CVSS calculator and severity metric at organizational level.
- Knowledge in Government of India guidelines for procurement of cloud services
- Experience in conducting Cyber Drills with red team, blue team and purple team exercise.
- Implementation of Information Security Awareness programs
- Experience in incident handling
- Experience in E-tendering and Government E Market (GEM) for Cyber Security Solutions procurement and vendor management
- Experience in Leading and Managing Information Security Audit for Application and Infrastructure
- Hands-on experience in implementing Cyber Crisis Management Plan as per CERT-In Mandate
- Experience in conducting compliance audit for KUA/AUA as per UIDAI guidelines
- Experience in ensuring Cyber forensics readiness, cryptographic requirements
- Hands-on experience in offering Managed Security Services

- Experience in Leading and Managing Information Security Audit for Application and Infrastructure
- Hands-on experience in implementing Cyber Crisis Management Plan as per CERT-In Mandate
- Experience in conducting compliance audit for KUA/AUA as per UIDAI guidelines
- Experience in ensuring Cyber forensics readiness, cryptographic requirements
- Hands-on experience in offering Managed Security Services
- Experience in implementing Security Operations Centre on turn key basis
- Experience in implementing brand monitoring solutions.
- Experience in managing classified projects under Government of India
- Understanding of Secure Code review
- Understanding of CISO guidelines issued by Ministry of Electronics and IT, Government of India

Professional Experience 2001-2007

(i) Worked as Programmer at IHRD College of Applied Science Peerumade. (Under Govt of Kerala)

Nature of work.:

- Handling classes for B.Sc. Computer Science and PGDCA
- Project guidance for B.Sc. computer Science and PGDCA students.

(ii)Worked as Senior Programmer at IT Academy software Solutions Cherthala, Kerala (June 2001-June 2002)

Nature of Work

- Management of all activities of the centre.
- Application Software development
- Project guidance for MCA, B. Tech and B.Sc. computer Science of various universities.

(iii)Lecturer/HSST St. Francis Assisi HSS Arthunkal, Alleppey (Department of Higher Secondary Education, Kerala) (June 2002-June 2007)

Nature of Work

- Overall, In-charge of the computer facility and Software Development

Professional Experience 2007-2019 (CDAC Bangalore)

Major Research and Development/Funded Projects Executed as Team Member

- Design and Development Hardware Based Intrusion Prevention System, funded by MEITY as team member (2007-2010)
- Nationwide PKI outreach programme, as the core member and responsible for conducting 1/2/3 days symposia/workshops and 2 National Conferences (2008-2011)
- Set-up and Operation of Disaster Recovery site for CERT-In Government of India, as team member funded by CERT-In (2011-2012 June)
- Setup and operation of Disaster Recovery Site for Controller of Certifying Authority Government of India as team member and played the role of trusted member (2012-2019)

Major Research and Development/Funded Projects Executed as Project Lead/Project Manager

- National Grid Computing Initiative: Grid Technology Services for Operational Phase of GARUDA, funded by DEITY for the activities from CDAC Electronics City (2010-2013)
- Setting up of ICT Infrastructure for IMSP Benin, funded by DST and MEA Govt. of India (2015)
- Security Ecosystem for National Super Computing Mission (2017-19)

Major Consultancy/Security Audit/Cyber Forensics Projects Executed as Project Lead/Project Manager

- Deployment and ToT of Cyber security Solutions to NIA, Navy
- Conducting system study and vulnerability assessment and Generating Information Security Policy for BMRCL (2015-16)
- Digital Forensics Analysis of the web page defacement of the e-payment gateway of CANARA Bank website, funded by CANARA Bank as team member (2016)
- Deriving Cyber security Framework for National E-Governance Services Limited (2017-18)
- Security Audit for BSNL Broadband Network (2017-18)
- Compliance Audit of NeSL Data Processing system as per IBBI regulations (2018-19)
- Infrastructure Audit for SRLDC (2019)
- Web Application audit of Applications in various domains (More Than 30 organizations)

Major Corporate Training Programs Executed as Project Lead/Project Manager

- Executed and delivered corporate training Programs in the area of Cyber Security to various organizations including:
    - IDRBT,MTNL, STQC, BEL, NTRO, Canara Bank, SRLDC, Indian Navy

ISO Management Representative and QMS manager

- Responsibility for Development and maintenance and Admission Management System and Payroll (In-house)

First QMS manager for ISO certification related activities of CDAC Electronic City and played a major role in getting the centre ISO certified

Professional Experience 2019-Till Date (CDAC Thiruvananthapuram)

Major Roles Carried out (2019-2021)

- Managing a 18-member team working as Security analysts and Information Security auditors
- Role as member Core Information Security Group supporting CDAC Top Management
- Played key role in setting up India's first Security Operation Centre in the government sector to offer Managed Security Services
- Lead Role in Offering Managed Security Services to JNPT and Kerala State IT Mission
- Project Lead for Security Audit and AADHAAR compliance audit services
- Lead Role in Carrying put incident analysis services.

Role as Member Core Information Security Group (3 Member Team)

- Responsible for implementation Cyber Crisis Management Plan across CDAC centres as per MEITY directions
- Preparation of IT Contingency Plan
- Preparation and implementation of Cyber Crisis Management Plan as per CERT-In mandate
- Preparation of incident response management and support for forensics analysis
- Preparation of cyber security advisory based on emerging threats
- Planning of ISMS implementation framework
- System study towards ISMS implementation
- Responsibility towards authoring and reviewing various process, procedures, templates and guidelines document
- Completion of ISMS process implementation
    - Information Security Policy
    - ISMS manual
    - Information Security Governance document
    - Applicable legislation template
    - Need and expectation of interested parties
    - ISMS Management review Process
    - Procedure for corrective and Preventive Actions for nonconformance
    - Statement of Applicability template
    - IT Asset Management
- Input towards MEITY direction for identification of major executive actions during emergency situations
- Input towards Global Cyber Security Index
- Review of customized policies, procedures and guidelines CDAC Centres
- Ensuring compliance as per NCIIPC and CERT-In regulations
- Act as advisory to Nodal Information Security Officers of CDAC Centres

Managed Security Services to Jawaharlal Nehru Port Trust (24x7 Service)

- Integration of Threat Intelligence feeds
- Preparation of SOP for SOC
- Incident Response Management plan for SOC
- Coordination of Annual Infrastructure audit
- Implementation of service desk for Incident response

- Implementation of VERIS (Vocabulary for Event Recording and Incident Sharing) framework for incident sharing.
- Implementation of OSINT based threat Intelligence
- Deployment to Malware Information Sharing Platform for IOC sharing and threat Intelligence collaboration
- Setting of blue team lab using Metasploit and Kali Linux and Sandboxing setup
- Work allocation and shift plan for Level 1 Analysts

Consultancy for Setting up Security Operation Centre for Kerala State IT Mission and Offer Service

- Vendor Interaction
- Preparation of RFP and selection of qualified vendor as per Government norms.
- User Acceptance testing and offer 24x7 services

Security Audit and Aadhaar Compliance Audit under CERT-In empanelment as Project Lead

- Interaction and submission of proposals
- Overall technical coordination of the audit activities
    - Kerala University
    - National E-Governance Services Limited
    - Kerala Police
- Carry out AADHAAR compliance audit for KUA/AUA (Existing 4 clients)

Incident response and Forensics Analysis as Project Lead

- Incident Analysis for
    - Spices Board
    - NAMPET

Personal Details

- Age and Date of Birth: 44, 4th May 1977

Languages Known: English, Hindi, Malayalam, Kannada

DECLARATION:

I hereby declare that the above-mentioned information is correct up to my knowledge and I bear the responsibility for the correctness of the above-mentioned particulars.

Date: 24th July 2021

Place: Thiruvananthapuram Dittin Andrews